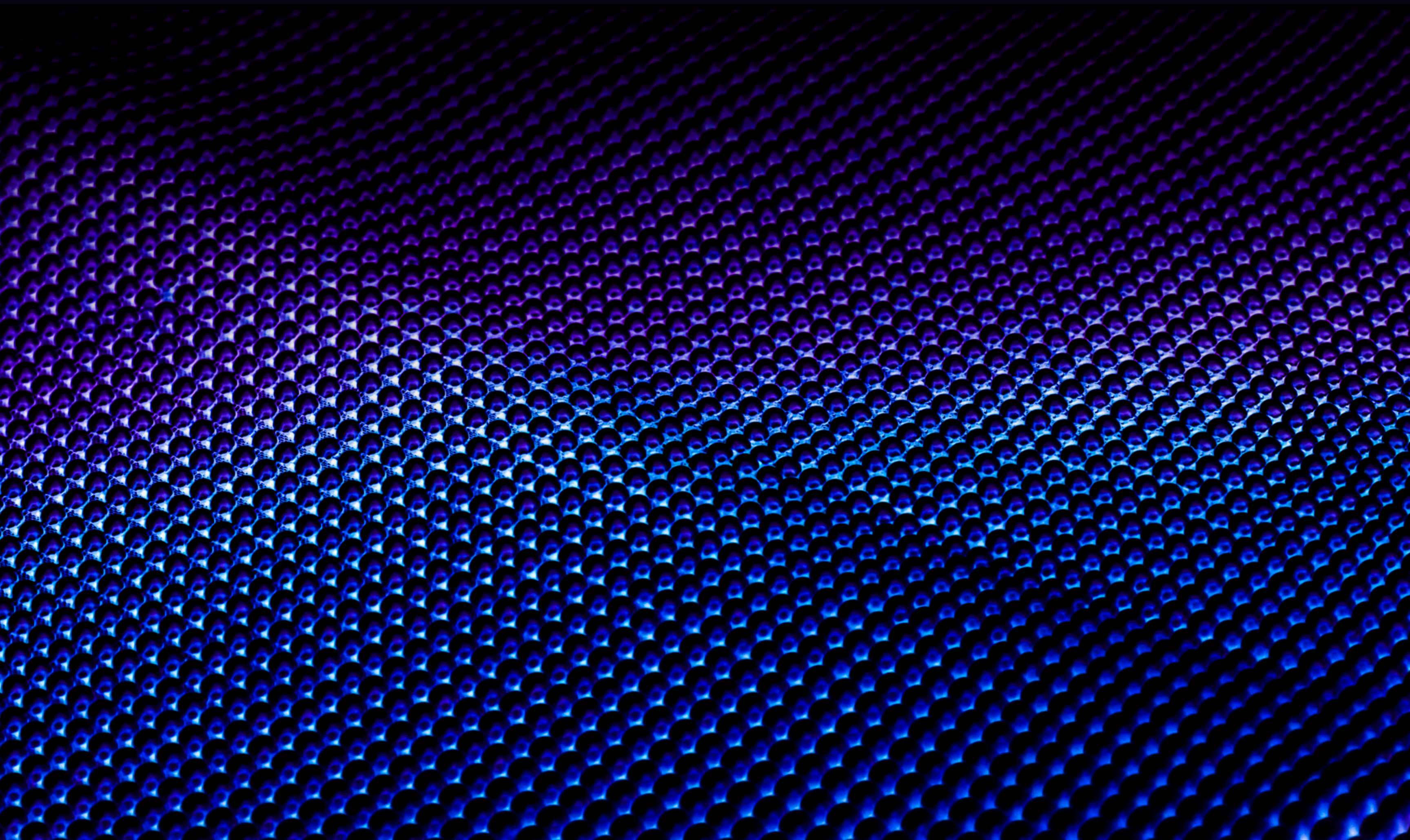
CISOS CONNECT™

CISOs INVESTIGATE: CYBERSECURITY DEBT

Peer-Authored Research



Thank you to our Corporate Partner

nagomi

—Promoting independent, vendor-neutral research for the benefit of the cybersecurity industry and a safer world at large

INTRODUCTION

BOB TURNER - EDITOR, CISOS INVESTIGATE: CYBERSECURITY DEBT

The concept of cybersecurity debt began as a collection of discussions in cyber circles around 2020. While no single definition has been agreed on across the cybersecurity profession, the concept of cybersecurity debt refers to the accumulation of neglected, outdated or insufficient security measures within an organization's IT infrastructure, processes or policies. In many ways, it is similar to the concept of technical debt, which describes the costs associated with cutting corners in software development, delaying technology refresh or failing to fix vulnerabilities promptly. Cybersecurity debt also happens through failure to invest adequately in security practices or people-centric items like security awareness for all users, and continued professional education for executives, managers and cybersecurity technologists. Cybersecurity debt can occur simply through delaying remediation of known risks due to resource constraints, or employees dodging security awareness training in favor of competing priorities.

Left alone, this debt grows, compounds, and eventually leaves the business vulnerable to cyber attack. Neglecting this cost of doing business on the internet can also compound the planning and effort needed to effect change, while increasing the cost of ongoing digital transformation or embracing artificial intelligence as a business success multiplier. Carrying cybersecurity debt on the books will increase the potential for catastrophic consequences such as data breaches, financial losses, regulatory fines and reputational damage.

I fully agree with our colleague Lock Langdon, the VP and Chief Information Security Officer at Aprio Advisory Group, LLC, who says:

“The CISO is responsible to identify and prioritize mitigation efforts accordingly. This is why CISOs exist!

The CEO's risk tolerance dictates the CISO’s threshold for managing cybersecurity debt. Critical risks that are unacceptable to the CEO are addressed first. Cybersecurity professionals must bridge the gap between technical vulnerabilities and business priorities, ensuring that cybersecurity debt is either remediated, mitigated or formally accepted by leadership.

These are difficult conversations. Much of cybersecurity debt accumulates because organizations lack clear risk articulation between technical and business leaders. A CISO's ability to communicate the cost-benefit relationship of cybersecurity decisions is vital. Trust in the CISO's rationale is essential for implementing necessary changes, yet reporting structures can sometimes distort or weaken the CISO's message to executive leadership.”

This report is not just the thoughts of one CISO. The authors of this report are all experienced Chief Information Security Officers from a variety of industries. Their wise counsel, experiences and valuable tips are worth your time to explore. Consider implementing their recommendations for your business.

Bob Turner

About CISOs Investigate

The value of peer input cannot be overstated. Authored by leading Chief Information Security Officers, CISOs Investigate is an ongoing series that offers firsthand insights to security leaders as they make business-driven risk and technology decisions.

CISO Contributors

CISOs Investigate: Cybersecurity Debt includes the viewpoints of 10 security leaders who have deployed or are looking to deploy third-party solutions. This report replaces the ad hoc, often informal and time-consuming processes of personally gathering peer insight. Spanning verticals, the CISO contributors share real-world use cases and provide guidance.

EXECUTIVE EDITOR:

Penn State University
Bob Turner
CISO

CONTRIBUTORS:

Hard Rock
Johann Balaguer
VP, Global CISO

GSR
David Cass
CISO

PGA TOUR Superstores
Alicia Clarke
Head of Cyber Security, Risk, and Privacy

RWE
Nikk Gilbert
CISO

Healthcare Industry
Monique Hart
Vice President of Information Security

World Vision USA
David Lackey
CISO

Aprio Advisory Group
Lock Langdon
VP & CISO

Healthfirst
Brian Miller
CISO

Belk
Neda Pitt
CISO

RWJBarnabas Health
Hussein Syed
CISO

WHAT IS CYBERSECURITY DEBT?

AUTHOR: LOCK LANGDON

Cybersecurity debt can define and quantify accrued security liabilities in an organization's IT, networks and technology. Similar to technical debt, cybersecurity debt builds as a company prioritizes short-term or quick-fix solutions over a sustainable IT and cybersecurity strategy.

What sets cybersecurity debt apart from technical debt is the all-important risk component. Although debt issues may overlap, cybersecurity's mandate is to focus on things from a risk perspective. That is the component that everything must be pinned to when identifying, prioritizing and categorizing cybersecurity debt.

Government regulations, like the new SEC regulations on reporting incidents, are setting higher floors for risk, adding must-do's above and beyond industry idiosyncrasies, risk tolerance, or financial ability to implement.

User behavior

A broad swath of user behavior contributes to cybersecurity debt. On one side are behaviors stemming from a lack of knowledge, inattentiveness, or a reluctance to tackle a complex upgrade. In the middle are people who accept that certain short-term security procedures must be done regularly to protect the organization. On the other side are malicious actors who don't want the application updated because they are exploiting weaknesses within it.

Many contributing behaviors to cybersecurity debt are industry-specific, because business drivers vary from sector to sector. In healthcare, it's acceptable to avoid the cost of replacing a very expensive legacy system with something more technically sophisticated as long as the old system still meets the patients' needs. In FinTech, advanced utilization of cutting-edge technologies that power more capability is seen as driving business.

Governments are funded by taxes, so debt scenarios revolve around budgetary cycles. Scrutiny around adding new technologies is high, and mandated criteria to win government contracts often add to cybersecurity and technical debt.

Increasing daily

Cybersecurity debt and technical debt can never be eliminated entirely. In fact, debt mounts with every passing day. More than 80% of debt scenarios have a budgetary component, but resource constraints exist, so it is the responsibility of the cybersecurity leader to identify risk and prioritize.

I set my threshold for cybersecurity debt around my CEO’s risk tolerance. Things that were extremely critical and too risky for the business leaders to accept are addressed first.

Need wins

Operationally, CISOs need wins under their belts to be able to go to bat for big institutional changes that might need to happen. This requires understanding the risk appetite of the leadership.

Good practices for articulating risk rest on what the CISO’s industry values. Healthcare values patient safety and availability above all. In a financial services organization, the top priority is client safety and driving value.

Small organizations can be more nimble because they can more easily articulate the risks and benefits. But their problem will be money. Big companies have a lot more stakeholder buy-in, and transitions are much more difficult because so much business process has been baked in over the course of years, if not decades.

> *“What sets security debt apart from technical debt is the all-important risk component. That is the component that everything must be pinned to when identifying, prioritizing and categorizing cybersecurity debt.”*

Sometimes it isn’t clear who in the organization owns the cybersecurity debt. Many business processes in human resources, for instance, live on top of technology. And sometimes a security fix is liable to break an application that the security team is not familiar with, so the problem isn’t redressed because roles are siloed.

Financial Debt vs. Cybersecurity Debt

Like a credit card balance silently growing in the background, cybersecurity debt accumulates in the shadows of every organization. Each postponed update, every skipped security review, and all those “we'll fix it later” decisions aren't just technical footnotes – they're unpaid loans against your company's future. And unlike financial debt, you won't know the interest rate until it's too late: when a breach turns that debt into a crisis that demands immediate payment.

Cybersecurity debt differs from financial debt because its impact depends on your organization's risk profile. You can't evaluate cybersecurity debt in isolation: It must be assessed based on how it could specifically harm your company.

Making things more complex, regulations like GDPR and HIPAA set mandatory security requirements that your company must meet, regardless of your risk tolerance or budget constraints. Security teams face a dual challenge: They must both protect against business-specific threats and ensure compliance with these strict regulatory frameworks, all while working within practical limitations.

Sources of Cybersecurity Debt

Cybersecurity debt arises from several common scenarios:

- **Expediency Over Quality:** Short-term solutions often bypass secure design principles. (CMU-SEI Congressional Report, 2023):
  - Using free code from an online GIT repo without checking for code vulnerabilities or flaws
  - Using default passwords across multiple systems to speed up deployment
  - Storing sensitive data in plaintext to avoid the complexity of proper encryption

- **Poor Design Choices:** Decisions made without adherence to best practices in validation and verification create lingering vulnerabilities. (Better Now Than Later, 2017)
  - Building custom encryption protocols instead of using established standards
  - Implementing direct database access without proper input validation, risking SQL injection
  - Using outdated authentication methods that are known to be vulnerable

- **Deferred Work:** Security patches and upgrades delayed for budgetary or operational reasons compound over time. (Better Now Than Later, 2017)
  - Running Windows server after end-of-life because upgrading is "too disruptive"
  - Keeping known-vulnerable third-party libraries in production code
  - Postponing critical firmware updates on network devices due to uptime requirements

- **Passing the Buck:** Organizations may offload cybersecurity debt onto users, customers, or maintainers. (Better Now Than Later, 2017)
  - Requiring end users to manage their own security updates on devices
  - Making employees responsible for self managing accounts and passwords
  - Assuming security responsibilities are managed by cloud providers

- **Time Pressure:** Strict production deadlines frequently result in security sacrifices. (Enterprise Information Systems, 2020)
  - Skipping penetration testing to meet a release deadline
  - Deploying code without proper security review due to urgent bug fixes
  - Rushing cloud configurations without implementing proper access controls

- **Lack of Standard Interfaces:** Poorly integrated components increase security complexity. (The Danger of Architectural Technical Debt, 2015)
  - Using multiple incompatible logging systems that create blind spots in security monitoring
  - Implementing different authentication systems across applications, leading to inconsistent security policies
  - Having multiple VPN solutions that can't share security policies or user management

Industry Specifics

Many contributing factors to cybersecurity debt are industry-specific because business drivers vary widely:

- Healthcare: Prioritizes patient safety and system availability
- Financial services: Focuses on client safety and value generation
- Higher education and research:
  - Diverse and data rich environments created with minimal documentation
  - Lack of resources for initial and continued risk assessments
  - Distributed governance of processes, technology and data
  - Creating new technologies where security is not primary interest
  - Speed of implementing specific technology for research projects, plus longevity of data-gathering systems
  - Minimal financial resources or flexibility
- Smaller organizations: More agile in risk-based decision-making but are often constrained by financial limitations
- Larger enterprises: Face complex stakeholder management and ingrained business processes that hinder rapid transitions

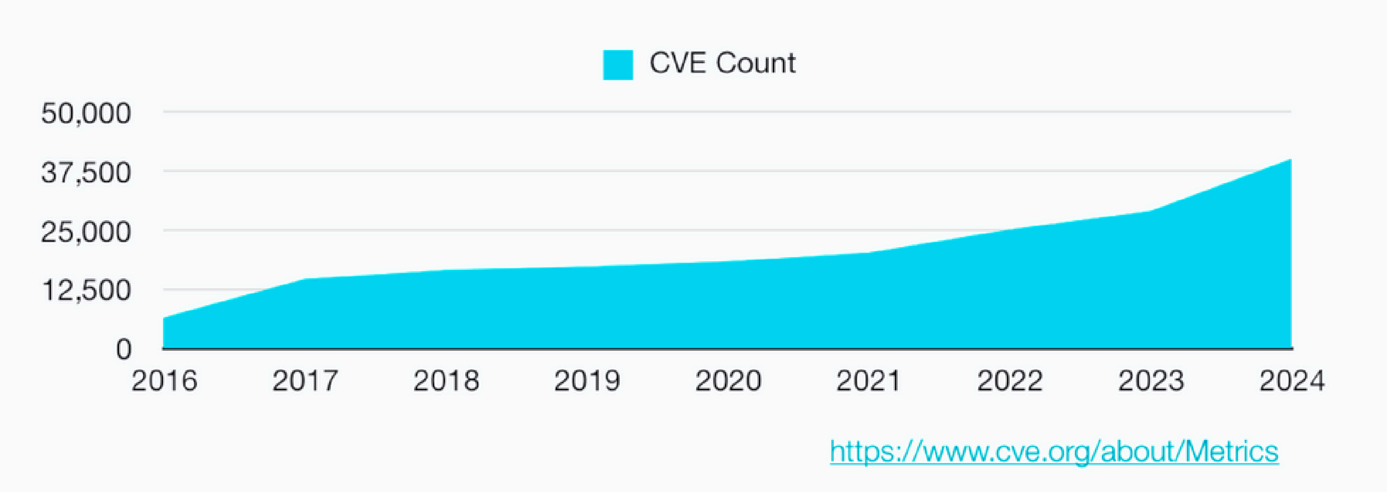
Mergers & Acquisitions, a Cybersecurity Debt Wild Card

Mergers and acquisitions (M&A) can often be a wild card due to their ability to increase cybersecurity debt quickly in multiple areas. When companies merge, they usually inherit a mix of legacy systems, outdated software and varying security practices, exposing your organization to numerous unknown vulnerabilities until an incident or other impactful event leads to a discovery. Integrating these disparate elements, especially under tight deadlines, can lead to shortcuts and compromises that result in a cybersecurity debt explosion. Be conscious of this and prepare budgets, staff and workloads accordingly.

Cybersecurity Debt at Large

Accenture, which conducted a study of government agencies, found that 85% of IT leaders believe not updating legacy technology could threaten their agency's future (Cybersecurity Debt: A Ticking Time Bomb!, 2021). Cybersecurity and technical debt are inescapable; they grow daily.

One of the most visible indicators of cybersecurity debt in our industry is the exponential growth of Common Vulnerabilities and Exposures (CVEs). Government agencies and public companies now dedicate entire teams to calculating the criticality of vulnerabilities, yet many remain unresolved due to fundamental design flaws that cannot be easily fixed.



https://www.cve.org/about/Metrics

While CVE scores help organizations prioritize risk, the sheer volume of vulnerabilities makes complete remediation impossible. Organizations with larger budgets and security teams can address more issues, but no entity can eliminate all vulnerabilities.

HOW DID WE GET HERE?

AUTHOR: BOB TURNER

IIn this section, clear your minds and take a good look at the business processes and security controls you already apply. Which of them result in materially reducing risk?

The authors of this report are united in our belief that cybersecurity debt is a significant issue born from nearly three decades of operating at risk. The past 25 years show improvement in short sprints, not a steady increase in following guidelines and applying and maturing reasonable sets of cybersecurity controls. The ebb and flow is punctuated by periods where leadership did not prioritize cybersecurity. This could cause employees to view cybersecurity as optional whether the discussion involves technical, procedural or political motivations. Their creative motivation is lost.

Perhaps that is the real issue -- apathy shown by many at the dawn of the cybersecurity age may have stifled creativity, as well as slowed progress in maturing cybersecurity controls and protocols. We have all heard that cybersecurity is hard, and implementing reasonable controls is seen as “overkill” for many organizations. More generously, some say cybersecurity is no longer a practice by professionals, it is more like “busy work.” With each new technology or process, we seek to balance optimism with diligent testing and validating of security controls. Optimism does not stop the hacker; well-engineered security controls and rapid response by taking immediate action does.

This never-ending accumulation of cybersecurity debt is a key contributor to CISO burnout. Security leaders operate under constant pressure, knowing they will never eliminate risk. They are tasked with managing an ever-expanding attack surface, facing the reality that vulnerabilities will continue to emerge faster than they can be addressed, all while needing to justify budgets, headcount and their team's necessity in the absence of significant security incidents.

This not only impacts information systems of business critical importance. Our colleague Hussein Syed, a longstanding CISO in the healthcare sector, believes the burned-out CISO tends to neglect those “easy-to-protect” systems that support non-data systems like alarms, environmental controls, building access and camera systems that fall within the boundaries of IT/OT.

The same challenges exist where the organization outsources components of cybersecurity. Johann Balaguer, an experienced cybersecurity leader in many industry sectors (and a former Marine), believes introducing a third party into your business operations inherently adds risk. While necessary in many cases, the inherent cybersecurity debt we get from third parties requires an intense focus from your CISO.

IT/OT CONVERGENCE

AUTHOR: HUSSEIN SYED

Operational technologies (OT) is a term used to encompass the systems, sensors and devices used to manage non-IT based operations, such as building control systems and production lines. Traditionally, systems were set up as standalone or on dedicated networks. The convergence of IT and OT technologies due to the digital transformation of enterprises to capture real time data for enhanced management and monitoring has increased the attack surface. OT technologies have a longer life cycle management than IT technologies and were not built with cybersecurity or privacy in mind, inherently presenting a risk to organizations. These systems are used to manage some of the most critical operations, and can even present an existential threat to an organization.

The universe of OT is quite large, ranging from industrial control systems (SCADA), building management systems (BMS), physical security systems (CPS) and manufacturing management systems (MMS). All these systems are networked to manage and monitor these environments. Weakness in these systems can be leveraged to disrupt operations through cyber attacks. These weaknesses can be default configurations, outdated and vulnerable software. In some cases, components are sourced through third parties with inadequate information to create the software bill of material (SBOM).

Each industry has its own unique, non-traditional IT technologies that help to run the business. They need to be accounted for, with risk management criteria developed based on how these technologies are utilized and how their life cycles play out. Some are replaceable. But sometimes the technology they want to replace it with hasn't been built to be secure because it was intended to run it in its own isolated system, and now it is to be run and controlled across centralized management areas. It will be placed on the network, where the technology will be exposed to exploitation. Every large enterprise has IT/OT risk; it's just a matter of how businesses are looking at this risk from a cyber risk perspective.

Case in point: Attackers compromised the surveillance camera system of a bank in Europe to monitor the movement of people, and capture typed-in passwords. They were able to very easily transfer funds out of that bank because the technology was either not secured or outdated.

Resiliency and Risk Management

Organizations should include OT technologies in their strategic plans of keeping these systems current. The risk management plan should include inventory of the networked OT technologies.

There are solutions available in the market that can identify these networked systems and classify them in categories so that respective ownership can be assigned. These systems can also create a configuration management database (CMDB) so that organizations can identify the cybersecurity debt of these systems. Next, stratify the risk as critical, high, medium and low to report to the leadership on where the risk lies and its potential impact. This provides the leadership or risk committee justification to allocate funding and resources to mitigate the risk.

Selection and procurement processes should be standardized to ensure enterprise products are purchased to include vulnerability management such as patches and updates to keep the systems current.

> *"The convergence of IT and OT technologies due to the digital transformation of enterprises has increased the attack surface. OT technologies have a longer life cycle management than IT technologies and were not built with cybersecurity or privacy in mind. These systems are used to manage some of the most critical operations and can even present an existential threat to an organization."*

The other challenge outdated OT systems present is that the outdated OT technology may not be built for newer IT technologies, creating a debt on the IT system. The IT systems, meanwhile, cannot be replaced because the application of the system it needs to support is not designed for newer IT technologies, compounding the IT risk.

Right context

Sometimes the leadership is not apprised of the risk in the right context, so it is unable to take an informed decision. If facilities management were to ask to replace an outdated building control system, executives might be disinclined to do so if it were still functioning. But if the same assessment of the system were to include the cyber risk and the risk of a disruption that could impact the business, then perhaps the leadership would look at that dated system differently, through the lens of reputational, regulatory or financial risk.

We need to break down silos and develop a working relationship with various business units so they can all jointly assess risk. Leadership in those business units will then be accountable for that risk, and in the event of an incident or disruption, it will be up to them to own the blame.

A better support model should be defined based on the organizational structure to report and manage risk. Cybersecurity can help quantify the cyber risk to the business line owner. The ownership for resiliency should be with business units to justify a decision to update, replace, or keep, with support provided by cybersecurity.

Operational Technologies vs Information Technologies

Feature	Operational Technology (OT)	Information Technology (IT)
Definition	A term used to encompass the systems, sensors and devices used to manage non-IT based operations	Technology used for data processing, storage and communication
Purpose	Provide management and monitoring of production lines, environmental systems, etc. Examples: BMS, SCADA systems, sensors, cameras, card access systems	Managing business data, cybersecurity, and enterprise applications. Examples: servers, storage, networking equipment, cloud infrastructure, enterprise resource planning systems
Connectivity Protocols	Use proprietary protocols or operate on segmented networks Are being converted to IP-based networks or communicate via gateways	Use TCP/IP communications protocols
Importance to Operations	Required to be available 24x7x365 Failure can result in production lines stoppage, environmental issues, physical security risks. May also present cyber risk if connected to the networks. Present strategic, financial and reputational risks	Failure can result in financial losses and/or service disruptions. Unmanaged (patching or updates) can result in cyber risks and intrusions. Present strategic, financial and reputational risks
Life Cycle Management and support	System updates are dependent on functionality requirements, narrow function design. Dependent on IT systems for management. Proprietary support models Life cycle of 10 to 15 years	Updated for bugs, security vulnerabilities and functionality Life cycle of 5 to 10 years

OUTSOURCED IT/CYBERSECURITY

AUTHOR: JOHANN BALAGUER

The high cost of security systems and the shortage of skilled talent make outsourcing an attractive option for many companies. In some cases, funding and staffing constraints necessitate outsourcing a significant portion of their security capabilities, or even entire security departments. However, buyers need to be aware.

Maintaining certain security functions within an organization can be very expensive. A security operations center, for example, requires a large staff to actively monitor, detect, and respond to threats around the clock, 365 days a year. This necessitates team members and leaders positioned globally, which incurs substantial costs. For organizations managing high levels of risk, outsourcing this function might be the best solution. A security service provider can offer comprehensive services, including telemetry and metrics from other organizations that feed into their central security operations, potentially benefiting your organization. Additionally, there are models where organizations can receive on-call support from a third party after hours.

When partnering with a provider, that third party is responsible for meeting SLAs and delivering on their commitments. However, if these third parties are located overseas, time zone differences can complicate collaboration, potentially affecting SLAs, goal achievement and deliverables.

Outsourcing can also exacerbate cybersecurity debt if the third party's security measures are not as robust as they claim. There is also the risk of intermixing information and data from the provider's various customers. Introducing a third party into your business operations inherently adds risk. This is a risk-based decision that organizations must make when deciding whether to fund a fully functional security operations center or outsource it to a third party.

Effective governance and oversight of any outsourced operation are crucial. The security team must establish SLAs, key performance indicators and metrics. Regular meetings with the leaders of the third party and its staff are essential to continuously fine-tune the service to meet your needs.

Constant touch points are critical. Do not assume the third party is always acting in your best interest. You need to be able to fail fast because prolonged recovery from a failure is not an option.

Discuss key points of contact and determine escalation paths. At what point should the third party alert the CISO versus issuing a general alert? Adversaries constantly change their tactics and techniques, so security leaders must calibrate their decisions and monitoring capabilities to ensure they are detecting the right activities.

> *"Outsourcing can exacerbate security debt if the third party's security measures are not as robust as they claim."*

Staffing a large development team is challenging, so development is often outsourced to different parts of the world where it is less costly and can be performed during off-hours. This may lead to faster delivery of upgrades, updates or enhanced system changes, but it also introduces risks related to code quality and vulnerabilities.

Moreover, there is extensive code reuse today, and no one truly knows what lies behind the millions of lines of open-source code. A security organization therefore needs the right quality assurance checks and technologies to scan for defects and security issues, as these can lead to cybersecurity debt.

Many out-of-the-box commodity solutions are available, but custom-tailored solutions might also be necessary, depending on the type of organization and industry vertical. A hybrid approach works well because many security components are fundamental to every organization. However, since each organization is unique, it is often necessary to develop custom-tailored capabilities, solutions and services to address the organization's specific operations and challenges.

THE UNSEEN CONSEQUENCE OF DIGITAL TRANSFORMATION

AUTHOR: DAVID LACKEY

As organizations embark on or complete their digital transformation journey, they often find themselves burdened with an unanticipated form of cybersecurity debt. This debt arises from failing to recognize and address the profound cybersecurity challenges of a digitally transformed world, where data, services and workforces are decentralized and highly distributed.

In this new paradigm, traditional security tools and approaches that once sufficed for centralized, on-premises environments are proving inadequate. Legacy solutions often lack the scalability and flexibility required to secure modern SaaS applications, cloud-native architectures and interconnected systems. The result is a patchwork of tools and processes that struggle to provide comprehensive visibility, governance and control across a sprawling digital ecosystem.

Security Implications of Digital Transformation

Organizations commonly fail to understand the cybersecurity implications of digital transformation. They mistakenly assume that existing security controls can be adapted with minor adjustments, when in reality, effective cybersecurity in a digitally transformed world requires a fundamental shift in strategy. Security teams need to adopt new tools and frameworks specifically designed for dynamic, decentralized environments, while building governance models that align with the new reality of digital business operations.

Without a strategic shift, organizations risk compounding their cybersecurity debt, leaving themselves vulnerable to emerging threats, data breaches and regulatory scrutiny. Addressing this challenge requires proactive investments in scalable security solutions, enhanced governance practices, and a commitment to aligning cybersecurity strategy with the organization’s operational priorities.

When a company plans to undergo digital transformation, security leaders need to be part of the conversation early on. They should define the cybersecurity consequences and governance-risk-compliance (GRC) implications, and articulate a clear vision that aligns with the organization’s objectives. Early engagement allows for better prioritization, informed decision-making and proactive budget planning to ensure the organization remains secure throughout its transformation.

Neglected Best Practices: A Growing Cybersecurity Debt Concern

Another critical contributor to the accumulation of cybersecurity debt lies in the neglect of configuration best practices. In their eagerness to innovate and deploy new capabilities, many organizations lose sight of the foundational elements of cybersecurity hygiene. This oversight often stems from a hyper-focus on rapid implementation, leaving configurations incomplete, inconsistent or misaligned with industry standards.

Compounding this issue is the dual role of operations and engineering teams in many organizations. These teams are tasked with both building and maintaining infrastructure and deploying new technologies. As a result, their focus frequently shifts to the demands of innovation and deployment, causing them to overlook the maintenance and optimization of tools and technologies already in use. This creates a cascading effect, where outdated configurations and neglected security tools further deepen the organization’s cybersecurity debt. As innovation and deployment demands increase, these teams lose focus on the security posture of already deployed tools, leading to:

- Misconfigured security controls
- Outdated or unpatched systems
- Weak or inconsistent enforcement of security policies
- Lack of continuous testing and validation

Over time, these gaps widen, increasing cybersecurity debt and fostering a false sense of security with capabilities already deployed, while hidden vulnerabilities persist unchecked.

Back to Basics: A Structured Approach to Reducing Cybersecurity Debt

To combat this accumulation of cybersecurity debt, I have implemented a shared annual initiative across all teams called "Back to Basics." This program ensures that configuration reviews of technology and security tools are a formalized goal each year. The initiative is designed to test, validate and optimize security capabilities through structured assessments and exercises.

Key components of Back to Basics:

- Annual security tool effectiveness reviews: Ensuring tools are properly configured, aligned to security standards, and actually working as intended.
- Security validation exercises: Testing security controls through real-world attack scenarios to identify misconfigurations or weaknesses.
- Process and responsibility alignment: Making sure every person, every process and every tool has a plan to ensure resilience and reduce operational risk.
- Reducing unnecessary complexity: Eliminating redundant, underutilized or poorly integrated security tools that contribute to operational inefficiencies.

Neglecting best practices and operational hygiene may seem like a minor issue, but over time, it creates a backlog of vulnerabilities that can quickly escalate into major security incidents. By making configuration validation and optimization a structured, deliberate process, organizations can proactively mitigate cybersecurity debt, strengthen their defenses, and lay a robust foundation for future growth.

Shared Security Goals: Embedding Security into Every Team's DNA

One of the most effective ways to ensure that security is a continuous priority across the organization is by implementing shared security goals for each team. This approach ensures that every team, not just security teams, is accountable for security within their respective areas.

By embedding security objectives into broader team goals, organizations can create a culture where security is an integral part of daily operations rather than an afterthought. This means security is not just a responsibility of the cybersecurity team but is owned across engineering, operations, development and business units.

> *"Cybersecurity debt is a growing challenge for organizations undergoing or post-digital transformation. Addressing it requires a shift from reactive security measures to proactive strategies that prioritize governance, configuration best practices, and shared accountability across all teams."*

Key Aspects of Shared Security Goals:

- Aligning security with delivery goals: Security should be part of how teams measure their success. For example, a "clean delivery" goal should also mean "secure delivery," ensuring that products and services are built with security in mind rather than as an add-on.
- Defining security ownership within teams: Each team should have clear security objectives tailored to their function, whether it's secure coding for development teams, secure configurations for IT teams, or incident response readiness for operations.
- Regular security reviews and accountability: Security goals should be measurable and reviewed periodically to ensure they are being met. Metrics can include vulnerability remediation times, adherence to security best practices, and effectiveness of security tools.
- Empowering teams with security knowledge: Organizations should invest in ongoing security education, hands-on training, and collaboration between security and engineering teams to help all employees understand how security impacts their work.

By integrating shared security goals, organizations can dramatically reduce cybersecurity debt by ensuring security is always a priority, rather than a secondary concern addressed only after an incident occurs. This approach fosters a proactive security mindset, enhances resilience, and ensures that security is a core component of business success.

Conclusion: Reducing Cybersecurity Debt Requires a Holistic Approach

Cybersecurity debt is a growing challenge for organizations undergoing or post-digital transformation. Addressing it requires a shift from reactive security measures to proactive strategies that prioritize governance, configuration best practices, and shared accountability across all teams.

Organizations that fail to recognize the security implications of digital transformation will continue to compound their cybersecurity debt, leading to increased risk exposure, compliance challenges, and weakened defenses against emerging cyber threats.

By embedding security into every team's goals, enforcing configuration best practices, and continuously reviewing security tool effectiveness, organizations can reverse the cycle of accumulating cybersecurity debt and establish a strong, scalable and resilient cybersecurity foundation for the future.

THE VALUE PROPOSITION

AUTHOR: BOB TURNER

While some CISOs fear the audit outcomes, the completion of the audit process reveals opportunities to retire or reduce cybersecurity debt. The minimum level of success is when audit findings validate effectiveness of current security controls, or improve cybersecurity technical processes. Value-added outcomes that offset cybersecurity debt are identification or confirmation whether policies and processes support further investment in infrastructure, introduction of new technologies, improving staff knowledge and performance, and recommendations for process development.

Process Optimization from Audits

Cybersecurity auditors frequently point to opportunities for process optimization across departments. The audit should identify ineffective threat mitigations and propose changes. Engage with your auditor to clarify all recommendations and for help in prioritizing corrections, changes or mitigation strategies.

Improved Security Posture

Continued evolution in cyber threats means there are always opportunities to improve your organization’s security. Beware of complacency and do not dismiss audit feedback. Improvements offset cybersecurity debt.

Operational Efficiency

Regular assessment of current and residual cybersecurity risk can be manual or automated. Automating your organization's protocols by incorporating continuous monitoring and improvement produces operational efficiency.

Enhanced Customer and Partner Trust

Cybersecurity programs must operate in the sense of trust developed through shared goals and regular assessment of people, process and tool effectiveness. The ability to confirm event information from shared investigation and forensic analysis of cyber events reflects on the skills of the team and dedication to materially reducing risk.

Regulatory and Legal Benefits

Measuring the value of cyber event data collected throughout pays off when capturing indicators of compromise and analyzing key events. Using the appropriate industry benchmarks, learn and compare the capabilities of your teams and tools. Are you using the best data provided?

> *"Continued evolution in cyber threats means there are always opportunities to improve your organization's security. Beware of complacency and do not dismiss audit feedback. Improvements offset cybersecurity debt."*

Long-Term Cost Avoidance

Knowing your team is ready partially depends on your current tools and processes. Synchronizing the tool outputs with risk assessment policies requires care, and can be measured through responses from review of Penn State Office of Cybersecurity security awareness messages. Share the latest risk analysis internally and make sure attack vectors and impact are understood across the organization.

Impact on Cybersecurity Liability Rates

Risk transfer by using tools like cyber liability insurance is influenced by the need to mitigate loss attributed to cybersecurity debt. Investing in cyber liability premiums with those investments backed by leadership and constituents partially depends on your current tools, policies and processes. Synchronizing the cybersecurity programs with risk assessment policies requires care and timing. Ensuring the organization, from the boardroom to the firewall boundary, relies on a corporate-wide understanding of how cybersecurity debt should be mitigated directly influences availability and overall cost of cyber liability insurance.

CALCULATING CYBERSECURITY DEBT

AUTHOR: BRIAN MILLER

Cybersecurity debt can be calculated by reviewing your tool landscape to ascertain which tools are being used and whether they are working together effectively. Debt calculation also involves an examination of hardware and software that is end of life, and can cause operational downtime to the business as well as a great deal of risk to security and to budget.

Security chiefs can approach cybersecurity debt through two lenses: quantitative and qualitative. Many CISOs lead with how much money the company will save through debt reduction. I prefer to lead with the business value that debt alleviation drives, and use the numbers to support that. Business value is what decision makers care about.

Think of it in these terms: You can tell someone that installing a seatbelt will ensure your family survives a high-speed car crash, or you can tell them what the components of that seat belt cost. The message that everybody will remember is that your family is going to survive, and then they look at the numbers and are reassured that you're not just selling vaporware.

Factors that increase or reduce cybersecurity debt

Cybersecurity debt is an outcome of security ineffectiveness. An investment has been made, but it is not delivering the expected outcome, either because systems are outdated, or tools are not operationalized correctly. The actual outcome is that you are paying too much for some things, and not paying for something else that's more valuable.

A good security program, therefore, needs to be measured in terms of effectiveness, as defined by context, and efficiency, which is delivering maximum financial value to the business and its customers.

The two really go together. I always go to the board and try to demonstrate that part of my strategy is to be fiscally responsible, prudent with my investments. For everything I buy, I try to decommission one or two things if I can. That makes my program effective and my finances efficient.

Strategically speaking, the aim is to identify tools that aren't being used or overlap, and thereby help to minimize risk to the business from a security perspective. This will also help to rationalize software overall, and that can be tied to security and business value.

Tools like FAIR™ (Factor Analysis of Information Risk) give us an outside-in view of enterprise risk and assign a top-level number. That number allows me to tell a story at a board level about where our risk lies, and what the range of numbers is. The numbers help us get to a story that says, here is the value we will get out of a particular tool.

> *"There are two lenses through which security chiefs can approach security debt: quantitative and qualitative. Many CISOs lead with how much money the company will save through debt reduction. I prefer to lead with the business value that debt alleviation drives, and use the numbers to support that. Business value is what decision makers care about."*

But the outside-in view only delivers a small part of the picture because it doesn't map the internal network of identity, endpoints, etc. As an industry we have not set a standard for assessing effectiveness and risk from the inside out. Many teams build their own systems, trying to stitch together a picture, but they fall short. Shifting toward a 360-degree, inside-out view will help security organizations tell the strategic risk story, and what can be done to redress it.

The biggest advantage the inside-out approach affords is that it focuses on things security teams can control, so we can reduce risk in a much more effective way.

A company will have hundreds of thousands of critical vulnerabilities. The vast majority will not be real because of all the controls in place. If I have a high CVE score, but the system is behind 16 firewalls and compensating controls and DLP, etc., then that scoring model doesn't work anymore.

If all these vulnerabilities were real, then my stock would be on fire all the time. But it's not. We have multiple layers that actually reduce the risk. A security chief must be able to prioritize and identify what the real risks are, within the context of these controls. But getting the broader picture of the context is hard, causing ineffectiveness in prioritization, ineffectiveness in vulnerability management, and ineffectiveness in correctly prioritizing threat intelligence.

My board was gratified when I could show them how a tool helped us to identify the real vulnerabilities, because that was a story of business value. This is where you're going to get your ROI , by tying real issues to the outcomes you want.

The old CIA triad – confidentiality, integrity and availability -- is a good concept, but some of those old models are of limited use in today's world. We must make this great model more applicable, and focus on being effective and efficient.

It's either change or evolve. The industry needs to shift. We need to figure out, how do we measure effectiveness, qualitatively and quantitatively. I think system-based or business capability-based are other ways to look at what we're doing.

One of our challenges is to facilitate cross-department conversations, to bring other executives to the table when it comes to security and security effectiveness. I think we can help to move the needle on that if we couch things in terms of operational and business impact.

In conclusion, to understand cybersecurity debt, the CISO has to be comfortable determining the return on investment (ROI) gained from proper implementation of a cybersecurity tool, process or people.

If cybersecurity debt is the accumulation of security risks and vulnerabilities due to delayed, incomplete or insufficient cybersecurity investments, then the cybersecurity ROI must account for the savings gained through implementing the proper tools, processes and people. The security teams implementing those components for an organization must recognize the measures of effectiveness, and assign financial value to cybersecurity investments relative to the risks they mitigate or prevent.

> *"Cybersecurity debt can be calculated by reviewing your tool landscape to ascertain which tools are being used and whether they are working together effectively. Debt calculation also involves an examination of hardware and software that is end of life and can cause operational downtime to the business as well as a great deal of risk to security and to budget."*

CLAIMING A RETURN ON INVESTMENTS THAT OFFSET CYBERSECURITY DEBT

AUTHOR: NEDA PITT

Investments in cybersecurity are transforming the role of the Chief Information Security Officer by driving efficiency, enhancing security, and accelerating time to market for businesses.

By reducing ongoing costs, these investments enable organizations to allocate resources more effectively, leading to significant savings. For instance, automated security solutions can minimize the need for manual interventions, reducing labor costs and freeing up personnel to focus on strategic initiatives. This cost efficiency not only improves the bottom line, but also allows the CISO to demonstrate tangible financial benefits to the leadership and board, fostering a unified understanding of the value of cybersecurity investments.

Moreover, these investments help organizations comply with internal policies, contractual obligations, industry guidelines and government regulations. Compliance is crucial for maintaining the trust of stakeholders and avoiding costly penalties. By implementing robust security measures, CISOs can ensure that their organizations meet all necessary requirements, thereby safeguarding their reputations and financial stability. This alignment with regulatory standards also simplifies audits and reporting processes, making it easier for the leadership and board to monitor compliance and make informed decisions.

Lowering risk

Investments in cybersecurity also play a pivotal role in lowering risk by reducing the probability and impact of incidents. Advanced threat detection and response systems can identify and mitigate potential threats before they escalate, minimizing the risk of data breaches and other security incidents. This proactive approach not only protects sensitive information, but also reduces the potential financial and reputational damage associated with security breaches. By effectively managing risk, CISOs can provide assurance to the leadership and board that the organization is well-protected against evolving threats.

Finally, these investments enable organizations to pursue new opportunities and gain a competitive advantage in the marketplace. Enhanced security measures can facilitate the adoption of new technologies and business models, allowing organizations to innovate and expand their offerings. For example, secure cloud solutions can support digital transformation initiatives, enabling faster time to market for new products and services. By leveraging these opportunities, CISOs can drive business growth and profitability, demonstrating the strategic value of cybersecurity investments to the leadership and board. This holistic approach ensures that all stakeholders speak the same language, focusing on risk reduction and increased profitability as key drivers of success.

Key Drivers for Reducing Cybersecurity Debt

1. Cost Efficiency: Upgrading outdated security systems reduces maintenance costs and improves operational efficiency. This driver focuses on the financial savings achieved by replacing legacy systems with modern, automated solutions.

2. Compliance: Ensuring adherence to internal policies, contractual obligations, industry guidelines and government regulations. Compliance helps avoid fines and enhances the organization's reputation, contributing to long-term financial stability.

3. Risk Reduction: Lowering the probability and impact of security incidents through advanced threat detection and response systems. This driver emphasizes the financial and reputational benefits of preventing data breaches and other security incidents.

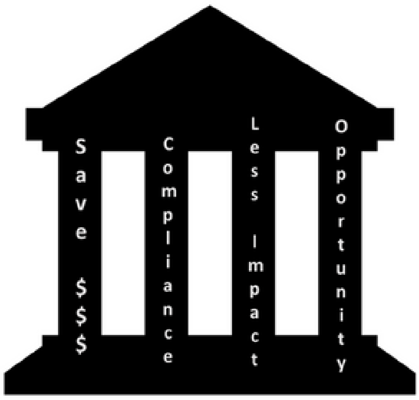
4. Innovation and Competitive Advantage: Enabling the adoption of new technologies and business models by securing the organization's infrastructure. This driver highlights the potential for business growth and faster time to market for new products and services.

In summary, addressing cybersecurity debt is essential for driving a robust ROI. By reducing ongoing costs, ensuring compliance, lowering risk, and enabling new opportunities, organizations can achieve significant financial and operational benefits. This holistic approach not only enhances security but also aligns with the strategic goals of the leadership and board, fostering a unified focus on risk reduction and increased profitability.

RETURN ON INVESTMENT

AUTHOR: BOB TURNER

Cybersecurity debt is not always about impending doom. Forbes noted that security executives are getting used to treating security as an investment in the future. Budgeting for cybersecurity tools and services is no longer an afterthought. Instead, today's CISO should be free to focus on returning value for the investment by demonstrating material reduction of risk. Cybersecurity debt can be a useful metric enhanced by calculating the expected return on that investment. Lower cybersecurity liability policy premiums is one part of that calculation. Forbes also proposed four pillars of cybersecurity ROI:



1. The investment saves money by reducing ongoing cost.
2. The investment helps the organization comply with internal policies, contractual obligations, industry guidelines or government regulations.
3. The investment lowers risk by reducing probability and impact of incidents.
4. The investment enables the organization to pursue new opportunities and gain competitive advantage in the marketplace.

Other logical discussions should take place when evaluating the value of cybersecurity investments. These may include calculating the cost of security testing, avoiding incident costs, and repelling the motivation to embrace the "shiny object syndrome" or making impulse purchases. Start by examining the organization's interests in buying the latest cybersecurity tools, technologies or innovative services. Before abandoning all reason to chase that technology, CISOs need to make clear connections between the purchase and the expected amortization for that investment.

The table below is a good start. In the following section, our colleague Neda Pitt, the CISO at Belk and a strategy-minded security executive, goes deeper into the many methods to calculate cybersecurity ROI.

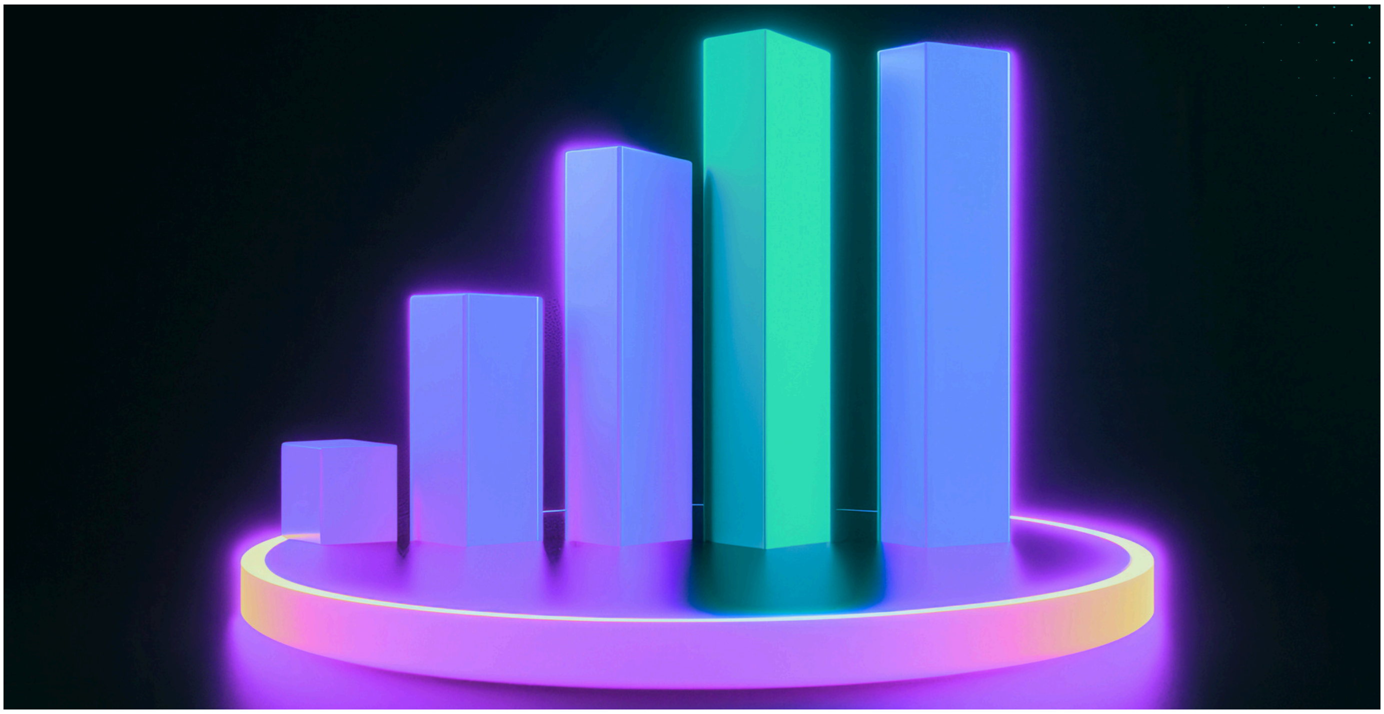
Issue / Strategy	Explanation and Impact
Cost of Proactive vs. Reactive Security	**Cost of Proactive Security** • Security tooling & technology costs • SIEM, EDR/XDR, firewalls, IAM, DLP, zero trust frameworks • Cloud security tools (CSPM, CWPP) • Personnel & training costs • Security team salaries, MSSP costs • Ongoing cybersecurity training & awareness programs • Compliance & risk management costs • Cost of audits, risk assessments, compliance adherence (e.g., SOC 2, ISO 27001, GDPR) • Incident prevention measures • Red teaming, penetration testing, bug bounties • Patching & vulnerability management programs **Cost of Reactive Security** • Breach containment & response costs • Downtime & business disruption • Regulatory fines & legal fees • Reputational damage & customer churn • Remediation & future security enhancements
Cost of Security Patching	**Cost of Patching (Investment in Prevention)** • Breach response & recovery costs • Development & patch costs (cost of fixing vulnerabilities later) • Operational downtime & productivity loss • Reputational & customer losses **Cost of Not Patching (Incident Response & Recovery)** • Unpatched vulnerabilities leading to ransomware attacks or system outages • Business disruption due to system remediation efforts • Reputational & customer losses • Customer churn due to lost trust • Stock price impact and brand reputation damage

Issue / Strategy	Explanation and Impact
Design Review Costs vs. Potential Security Breaches	**Cost of Secure Design Reviews (Proactive Investment)** • Personnel costs • Threat modeling tools (e.g., Microsoft Threat Modeling Tool, OWASP Threat Dragon) • Automated static/dynamic analysis tools for early vulnerability detection • Process & compliance costs **Cost of Not Conducting Secure Design Reviews (Reactive Costs)** • Breach response & recovery costs • Incident response, forensics, containment, and mitigation • Legal fees, regulatory fines (e.g., GDPR, CCPA, HIPAA) • Development & patch costs (Cost of Fixing Vulnerabilities Later) • Operational downtime & productivity loss • System outages due to security flaws • Ransomware recovery costs • Reputational & customer losses • Customer churn due to lost trust • Stock price impact and brand damage
Downtime Due to Security Incidents	**Lost Revenue** • Critical systems go offline **Productivity Loss** • Employee downtime due to unavailable systems **Incident Response & Recovery Costs** • Costs related to IT/security team response, forensic investigations, and system restoration • External consultant costs **Reputational Damage & Customer Churn** • Customers may switch to competitors if downtime affects trust **Regulatory Fines & Legal Costs** • Downtime incidents can result in fines (e.g., GDPR, SEC) • Costs include legal fees, audits, and settlement payouts
Reduced Remediation Costs	**Cost of Security Remediation (Reactive Costs)** • Incident response & containment costs • Forensic investigations, threat analysis, and containment efforts. • System patching & fixes • Emergency patching, reconfiguration, and code fixes due to exploited vulnerabilities. **Legal, Compliance & Regulatory Fines** • Non-compliance penalties from GDPR, CCPA, HIPAA, PCI DSS, SEC, etc. **Reputational Damage & Customer Loss** • Loss of customer trust, brand impact and PR crisis management. **Cost of Proactive Security Measures (Prevention Costs)** • Security automation (SIEM, EDR, SOAR, vulnerability scanning) • Patch management & hardening (automated patching, secure configurations) • Threat detection & response (MDR, XDR, penetration testing, red teaming) • Security awareness & training (reducing human error, phishing prevention)

Issue / Strategy	Explanation and Impact
Incident Response Costs	**Incident Detection & Investigation Costs** • Security team hours spent on detection and triage • Forensic investigations, external consultants, and threat analysis • SIEM/SOAR operational costs related to incident analysis **Containment & Mitigation Costs** • Immediate remediation efforts (e.g., isolating systems, applying emergency patches) • Incident response playbook execution, backup restoration **Recovery & Remediation Costs** • Restoring affected systems, reimaging compromised devices • Software/hardware replacements due to security failures **Legal, Compliance & Notification Costs** • Regulatory fines, legal fees, and compliance audits • Breach notification costs **Reputation Damage & Business Impact** • Customer churn due to breach impact • Lost revenue from downtime or operational disruptions
Cost of Security Training	**Cost of Security Incidents Due to Human Error (Reactive Costs)** • Phishing & social engineering attacks • Employees clicking malicious links or disclosing credentials **Insider Threats & Accidental Data Exposure** • Misconfigurations, accidental data sharing, or weak passwords **Compliance Violations & Regulatory Fines** • Non-compliance due to untrained employees mishandling sensitive data **Incident Response & Remediation Costs** • Costs related to forensic investigations, legal fees, and recovery efforts
Incident Prevention and Faster Recovery	**Cost of Preventative Security Measures** • Security tools & infrastructure • Incident response planning & DR/BCP • Security awareness & training • Compliance & risk assessments **ROI of Preventative Security Investments vs. Downtime Costs** • Total downtime cost • Preventative cost • Annual security investment (proactive measures) • Potential downtime cost due to security incidents

MEASURING ROI

AUTHOR: NEDA PITT



Addressing cybersecurity debt is crucial for driving a robust return on investment (ROI) for an organization. Cybersecurity debt refers to the accumulation of outdated or insufficient security measures that can leave an organization vulnerable to threats. By investing in modernizing and enhancing cybersecurity infrastructure, organizations can significantly reduce this debt, leading to multiple financial and operational benefits.

Firstly, reducing cybersecurity debt helps in lowering ongoing costs. Outdated security systems often require more maintenance and are less efficient, leading to higher operational expenses. By upgrading to more advanced and automated security solutions, organizations can reduce these costs, resulting in substantial savings. This cost efficiency directly contributes to a positive ROI, as the savings can be reinvested into other strategic areas of the business.

Secondly, addressing cybersecurity debt ensures compliance with internal policies, contractual obligations, industry guidelines and government regulations. Non-compliance can result in hefty fines and damage to an organization's reputation. By investing in up-to-date security measures, organizations can avoid these penalties and maintain the trust of their stakeholders. This compliance not only protects the organization financially, but also enhances its credibility in the market, contributing to long-term profitability.

Moreover, modernizing cybersecurity infrastructure lowers the risk of incidents by reducing the probability and impact of security breaches. Advanced threat detection and response systems can proactively identify and mitigate potential threats, preventing costly data breaches and other security incidents. This proactive approach minimizes financial losses and protects the organization's reputation, further enhancing ROI. By effectively managing risk, organizations can ensure business continuity and stability, which are critical for sustained growth.

ROI Calculation Methods

To measure the reduction of cybersecurity debt effectively, it's essential to use appropriate ROI calculation methods. See Appendix for a comprehensive set of ROI calculation methods and outcomes.

REPRESENTATIVE METRICS

AUTHOR: JOHANN BALAGUER

Effectively communicating cybersecurity debt and its associated risks to leadership and the board is crucial. Utilizing appropriate metrics is essential for conveying these concepts and aiding the business in developing strategic plans aligned with its risk appetite.

Unresolved cybersecurity debt heightens the risk of attacks and data exposure. Metrics play a vital role in risk management by helping security leaders explain and prioritize risks to non-technical leadership and boards. This, in turn, enables boards, enterprise risk management committees and security committees to make informed decisions based on heightened awareness.

> *"Effectively communicating cybersecurity debt and its associated risks to leadership and the board is crucial. Utilizing appropriate metrics is essential for conveying these concepts and aiding the business in developing strategic plans aligned with its risk appetite."*

One of the most significant debt items organizations face is end-of-life systems and software. Dashboards are invaluable tools in these scenarios. An effective dashboard not only displays current mitigations and controls but also projects upcoming issues five years in advance or longer. This foresight allows organizations to account for end-of-life expenses early and budget accordingly. The sooner an early warning indicator is triggered, the better an organization can forecast its budgeting needs.

Incorporating data and posture management into a dashboard also reveals how quickly systems are being updated to avoid end-of-life status, or whether extended security updates are necessary. These two key metrics help organizations decide whether to fund mitigation efforts, segment vulnerable systems, or decommission them altogether.

Various technologies can be utilized to understand the organization's risk posture. Common tools include vulnerability scanners and aggregators that compile information from different technologies to provide a comprehensive view of the risk landscape and identify where security debt resides. This data also aids organizations in their use of quantitative risk calculations, such as Factor Analysis of Information Risk (FAIR™) models, to assess the probability of impact.

End-of-life systems, as mentioned earlier, are a key risk indicator. Burndown rates are also crucial, as they help the security team track the effectiveness of debt consolidation efforts. This data provides leadership and boards with the insights needed to make well-informed strategic decisions.

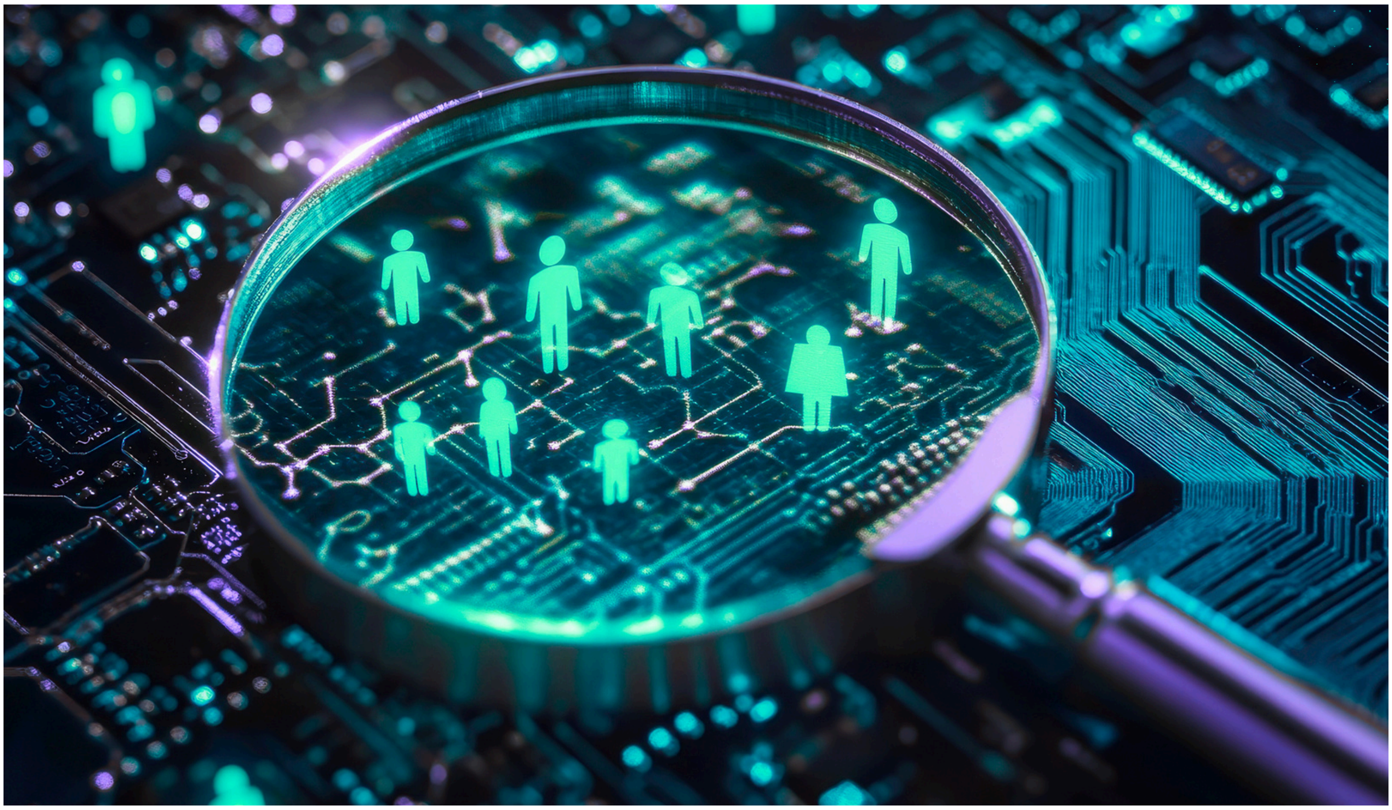
Linking these metrics to critical assets and the broader risks that vulnerabilities may pose to the organization helps non-technical stakeholders understand the potential business impact if a particular system fails. Leveraging these metrics is essential for strategic decision-making.

Vulnerabilities may exist outside the security team's direct control, hidden within various business units. Therefore, it is not solely the security team's responsibility to address all forms of cybersecurity debt. This responsibility varies, depending on the organization's type and structure. However, the security team must assist the broader organization in prioritizing the most significant risks. This information must be communicated to stakeholders across the business to enable judicious, priority-based decisions from both a lifecycle remediation and budgeting perspective.

Metric	Definition
Key Risk Indicators	
Early Warning Indicators	(e.g., EOL dashboards)
System Criticality	Identifying “business critical” systems (business loss and cost to recover from financial loss due to system unavailable)
Key Performance Indicators	
Unresolved Cybersecurity Debt	Business metrics that indicate cybersecurity debt, ideally equal to zero. Organizations should set the tolerance based on the cost to remediate technical debt.
Time to Resolve Technical Debt	Tracking technical debt resolution helps organizations maintain software quality, security, and operational efficiency.
Cost of mitigation strategies (tied to life cycle management)	Measures of cost to reduce risks, enhance security, and improve operational efficiency

IMPACT OF INADEQUATE TALENT

AUTHOR: ALICIA LAING CLARKE



Technical Staff Debt

The lack of adequately skilled, engaged, and efficient security practitioners within organizations significantly contributes to cybersecurity debt, which must be addressed through human capital development programs, flexible talent management and reducing burnout.

As breaches become more frequent and increasingly disruptive, addressing cybersecurity debt must involve technology, processes and people. The absence of the proper or sufficient talent can create debt across multiple areas, compromising security, hindering modernization and impeding business growth.

Cybersecurity faces a notable talent deficit, partly due to a lack of creativity in hiring practices. Many job advertisements inadvertently exclude promising candidates by setting high threshold requirements that few can meet.

The World Economic Forum's "Bridging the Cyber Skills Gap" initiative advocates for a "skills first" approach to create more flexible career paths and broaden the talent pool. This approach focuses on skills and competencies rather than degrees, job histories, and titles, making room for nontraditional and diverse talent with strong problem-solving skills, motivation, and a commitment to continuous learning—qualities essential for success in the field.

Attracting non-traditional and diverse talent to cybersecurity teams requires a thoughtful and up-to-date training program that capitalizes on their strengths and introduces them to various opportunities within the field.

Recruiters

Recruiters play a crucial role in bringing in the right talent, which depends mainly on their research, openness to hiring outside traditional norms, and ability to identify candidates with a strong willingness to learn and a natural aptitude for problem-solving.

Recruiting talent in an expanding threat landscape is challenging; retaining it is another. Retention demands that organizations provide upskilling and career development opportunities to keep security professionals motivated and focused on present challenges and those likely to emerge in the future. Employees take valuable knowledge with them when they leave, exacerbating cybersecurity debt. C-suite executives must understand the security and business implications of this talent shortage.

> *"The lack of adequately skilled, engaged, and efficient security practitioners within organizations significantly contributes to cybersecurity debt, which must be addressed through human capital development programs, flexible talent management and reducing burnout."*

Security professionals sometimes leave organizations as part of strategic business decisions, such as during company acquisitions, which may result in the termination of entire security teams. In such cases, if no documentation exists around the technology in use at those organizations, the loss of institutional knowledge can quickly escalate an incident into a crisis.Suppose security-related layoffs are part of a business strategy. In that case, organizations should prepare a roadmap to mitigate this debt, introduce new solutions that meet current standards, and hire the right people with the necessary training and knowledge to support the updated systems.

Due to overwork and mounting responsibilities, job stress can also contribute to security debt by discouraging new talent from entering the field, diminishing the effectiveness of existing employees, and leading to burnout. Increased resource allocation can help alleviate some of these issues.

Specific Talent Needed

While staffing levels are essential, they are not the sole factor. When a company experiences a breach, it may expand its security teams. However, this can inadvertently contribute to cybersecurity debt, as new hires must be trained and up to speed.

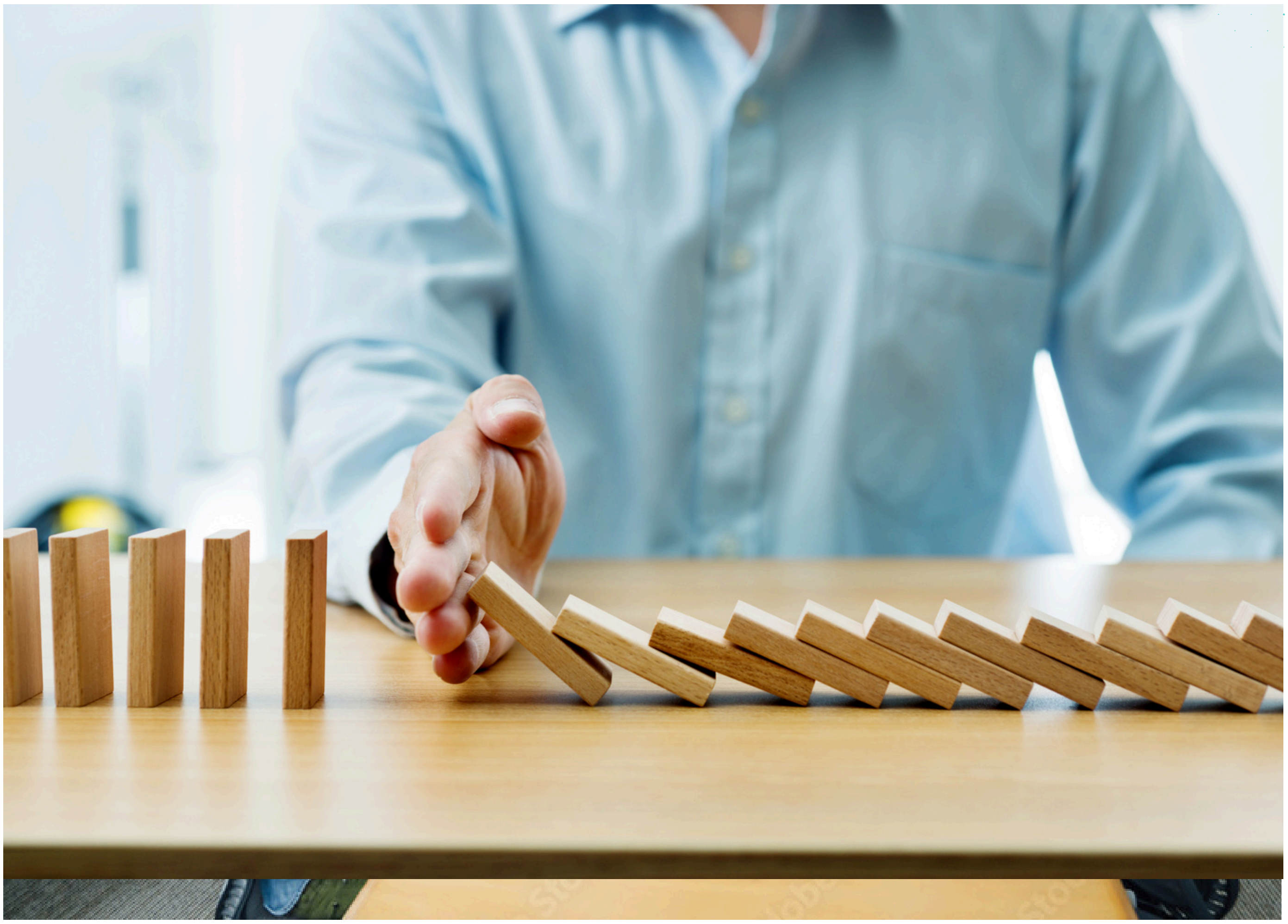
Talent should be assessed based on the number of staff and whether they possess the right skills to perform necessary tasks, support existing technology, and prepare for future technological advancements. Sometimes, this requires proper on-the-job training.

The extent of talent-related cybersecurity debt can vary by sector and organization type. For example, a growing public organization may have the funding to hire the necessary resources to enhance its effectiveness, while the same approach may not be feasible in other organizations.

The cybersecurity talent shortage is deepening cybersecurity debt, but a strategic approach can alleviate these challenges. Addressing this critical aspect of cybersecurity debt is essential to ensuring our organizations' and societies' safety and resilience.

HOW DO WE BREAK THE CYCLE?

AUTHOR: BOB TURNER



Far too often the CISO is called on to help create breathing room in the corporate IT budget. Creatively controlling the cost of purchasing technology, contracting services and maintaining and training cybersecurity staff is only part of the equation. CISOs must address the debt caused by accumulation of unresolved security vulnerabilities, lingering technical debt, or underinvested security initiatives that create long-term risk for their organization.

We rely on broad concepts like managing security culture, technology road maps, proactive risk management, strategic planning and cybersecurity awareness training with the hope that any effort is good effort in the ongoing battle.

Cybersecurity debt is unavoidable, but how organizations identify, categorize and mitigate it will define their resilience in an increasingly complex threat landscape.

Table 1 - Ranked Examples of Behaviors Indicating Cybersecurity Debt

Rank	Behavior
1	Delaying security updates
2	Failure to apply software patches, firmware updates or operating system upgrades in a timely manner
3	Using outdated technologies and legacy systems that are no longer supported or secure
4	Lack of budget allocation or insufficient funding for cybersecurity tools, personnel, or training
5	Prioritizing other business initiatives over cybersecurity improvements
6	Rapid expansion without security scaling
7	Adding new technologies, systems, or endpoints without integrating proper security controls
8	Ignoring security measures while adopting cloud computing, IoT or remote work solutions
9	Underestimating or dismissing known security risks as low-priority concerns
10	Taking a reactive vs. proactive approach: • Focusing solely on responding to incidents instead of preventing them • Implementing "band-aid fixes" without addressing root causes

(Note: Ranking provided by The Cyber Hero vCISO Network GPT powered by CyberShield)

No doubt those activities are part of the broader picture. Are they effective? What if we set our sights on relieving the pressure caused by dividing our focus between corporate politics, government regulatory oversight, and the ongoing technical and human challenges.

Delivering cybersecurity debt reduction requires asking and answering the hard questions. Here is a short list for getting started:

- Does your program build on risk assessment, reduction, then continuous monitoring with active response?
  - Identify - Prioritize - Remediate - Retest - Validate
- Is cybersecurity an investment or operational cost of doing business?
  - Review - Invest - Configure - Test - Implement
- Are you continually assessing our technology infrastructure using a diverse set of strategies?
  - Define - Discover - Evaluate - Analyze - Decide
- Are you calculating and addressing how to:
  - **Measure and reduce cost of compliance**
  - **Reduce human error** by automating processes and exploring, then implementing tools backed by artificial intelligence
  - **Manage vendor relationships** including cost and risk
  - **Address the debt** incurred through poor application of third party risk management
- Is your incident response program tracking meantime metrics for detection, containment and remediation?
- How do customers view your compliance program? Is it merely “security theater” or are you materially reducing risk (feel free to add “one system at a time” here)?
- Do you involve executives and board members in tabletop exercises for improving incident response, ransomware treatment, crisis response communications and program awareness?
- How often do you have conversations with executives, managers and IT teams on cybersecurity customer experience?
- Do you engage IT teams as strategic partners or as a group of technicians?

> *“Solving cybersecurity debt is a team sport. Excess cybersecurity debt impacts the ability to improve, innovate and dominate in the market, just like individual athletes neglecting their health will impact the team’s ability to dominate in the related league and sport.”*

Solving cybersecurity debt is a team sport. Excess cybersecurity debt impacts the ability to improve, innovate and dominate in the market, just like individual athletes neglecting their health will impact the team’s ability to dominate in the related league and sport. The suggestions above are a foundational set of exercises an organization must incorporate into pre-season training and then execute as part of the corporate game plan.

COMPLIANCE IS NOT SECURITY!

AUTHOR: DAVID CASS

Security is not the same as compliance. They work hand in hand, but plenty of companies that have been compliant with their regulator's directives still get breached.

Compliance usually focuses on a certain aspect of security, and in many cases speaks to minimum requirements that organizations need to adhere to. Don't let the fact that your organization is compliant make you complacent, because you're compliant with the bare minimum requirements at a time when the landscape is changing constantly. Compliance doesn't mean you're not vulnerable.

Moreover, compliance doesn't necessarily set the actual specific controls, because some regulators are principle-based while others are prescriptive. That first group would require something like "a process for managing privileged users." The second group would explicitly require multi factor authentication.

If you answer to regulators who are principle based, then it's upon you to prove how you're addressing the principle. There are probably a dozen different ways you could implement that, and how you implement it is important, because it has to be sustainable and scalable.

Other regulations are written in stone, so there's no avoiding what they prescribe.

It is up to the business to figure out what compliance regime it is beholden to, and then proceed from there. There are cases when a system isn't end of life, end of service from a compliance point of view, but it's no longer capable of meeting updates to compliance requirements. If it isn't meeting your needs to help adhere to the latest compliance regime, it's advisable to sunset that system and move on.

From a compliance point of view, regulators tend to focus on end of life and end of service. Once a system reaches that point, it's too late from a regulatory point of view, and the fines start rolling in. Even though manufacturers and vendors disclose the final warnings, many organizations are not vigilant about planning to refresh tech debt, whether cybersecurity-related or general portfolio. And many still don't do anything even after they have to start paying fines and buying extended service agreements.

If a business doesn't address cybersecurity processes, certifications or accreditations, then there could be more at stake than lost contracts. It may come back as a lawsuit, and the value of that lawsuit becomes yet another component of cybersecurity debt.

> *"Don't let the fact that your organization is compliant make you complacent, because the fact is, you're compliant with the bare minimum requirements at a time when the landscape is changing constantly."*

Each regulatory body has its own guidelines for how often they update the regulations. Most organizations should also be looking at the regulators' guidance, and not only their requirements or regulations, because guidance is usually the future predictor of how regulations are going to change.

From the perspective of cybersecurity debt, the real road forward is migration to the cloud and SaaS. For cloud-native organizations, tech debt, cybersecurity or otherwise, is fairly easy to deal with. When the SaaS product fails to continue meeting the organization's ongoing needs or something better comes out, it's quick to shift. And platforms like AWS or Google will only allow customers to get so far behind in their versions before they upgrade automatically. That's their hold-harmless clause, a means to avoid incidents that unfold because someone fails to upgrade.

ROI CALCULATION METHODS

AUTHOR: NEDA PITT

It’s critical to use appropriate ROI calculation methods to effectively measure the reduction of cybersecurity methods. Here are the ROI calculations to consider:

1. Return on Security Investment (ROSI):

- **Formula:** ROSI=Monetary Value of Risk Reduction−Cost of Security Investment / Cost of Security Investment×100%
- **Monetary Value of Risk Reduction:** The expected financial loss from cyber threats if no security measures were implemented.
- **Cost of Security Investment:** The total amount spent on cybersecurity solutions.

2. Annual Loss Expectancy (ALE):

- **Formula:** ALE=Single Loss Expectancy (SLE)×Annual Rate of Occurrence (ARO)
- **Single Loss Expectancy (SLE):** The financial loss expected from a single security incident.
- **Annual Rate of Occurrence (ARO):** The estimated frequency of the incident occurring within a year.

3. Cost-Benefit Analysis (CBA):

- **Formula:** CBA=Total Benefits - Total Costs
- **Total Benefits:** The sum of all financial gains from implementing cybersecurity measures, including avoided losses and operational efficiencies.
- **Total Costs:** The total expenses incurred for cybersecurity investments.

By focusing on these key drivers and using these ROI calculation methods, organizations can effectively measure the reduction of cybersecurity debt and demonstrate their cybersecurity investments' financial and strategic value. This approach ensures that all stakeholders, including leadership and the board, understand the importance of addressing cybersecurity debt and its impact on risk reduction and profitability.

ROI Metrics

Proactive Security ROI:

- Return on Security Investment (ROSI):
    - Formula: ROSI=Monetary Value of Risk Reduction−Cost of Security InvestmentCost of Security Investment×100%
        - ROSI=Cost of Security Investment / Monetary Value of Risk Reduction−Cost of Security Investment×100%
    - Key Metrics:
        - Reduction in the number of security incidents.
        - Decrease in downtime and operational disruptions.
        - Lower costs associated with incident response and recovery.
        - Improved compliance and reduced fines.

Reactive Security ROI:

- Cost-Benefit Analysis (CBA):
    - Formula: CBA=Total Benefits - Total Costs
    - Key Metrics:
        - time to detect (MTTD) and respond (MTTR) to incidents
        - costs incurred from data breaches and recovery efforts
        - impact on business operations and revenue loss
        - effectiveness of incident response plans and procedures

By comparing the ROI of proactive and reactive security measures, organizations can make informed decisions about their cybersecurity investments. Proactive security often provides a higher ROI by preventing incidents and reducing long-term costs, while reactive security is essential for mitigating the impact of unforeseen threats. Balancing both approaches ensures a comprehensive cybersecurity strategy that maximizes protection and minimizes financial losses.

$$\text{ROSI} = \frac{\text{reduction in risk ‘\$’ - cost of control}}{\text{cost of control}}$$

$$\text{Reduction in risk} = \text{Annualized rate of occurence} \times \text{Expected monetary loss for a single event} \times \text{Reduction in probability of risk occurrence with the implemented control}$$

ROI of Security Patching:

Security Patching: Security patching involves applying updates to software and operating systems to fix vulnerabilities and improve security. These patches are typically released by software vendors to address identified security flaws, performance bugs, or to enhance security features.

Regularly applying security patches is crucial for protecting an organization's digital assets from cyber threats and ensuring compliance with regulatory requirements.

ROI Metric for Security Patching

Return on Security Investment (ROSI):

- **Formula:** ROSI=Monetary Value of Risk Reduction−Cost of Security Patching
  - Cost of Security Patching×100%
  - ROSI=Cost of Security Patching
  - Monetary Value of Risk Reduction− Cost of Security Patching×100%

- **Monetary Value of Risk Reduction:** The expected financial loss from potential security incidents if patches are not applied.

- **Cost of Security Patching:** The total expenses incurred for implementing security patches, including labor, tools and downtime.

Key Metrics to Track

1. **Vulnerability Patch Time:** The time taken to identify and apply patches after a vulnerability is discovered. Shorter patch times indicate a more proactive security posture.
2. **Number of Unpatched Vulnerabilities:** The count of known vulnerabilities that have not yet been patched. Fewer unpatched vulnerabilities suggest better security management.
3. **Incident Reduction:** The decrease in the number of security incidents attributable to unpatched vulnerabilities. This metric helps quantify the effectiveness of patching efforts.
4. **Compliance Rate:** The percentage of systems that are up-to-date with the latest security patches. Higher compliance rates indicate better adherence to security policies and regulatory requirements.

By focusing on these metrics, organizations can effectively measure the ROI of their security patching efforts and demonstrate the financial and strategic value of maintaining an up-to-date security posture. This approach ensures that all stakeholders understand the importance of timely patching in reducing risk and enhancing profitability.

Design Review Cost vs Potential Security Breaches:

Design Review Costs: Design review costs refer to the expenses incurred during the evaluation of design work to ensure it meets specific goals and objectives. This process involves stakeholders reviewing the design to identify potential issues, align with project requirements, and make necessary adjustments before implementation. Effective design reviews help prevent costly rework, scope creep and project delays.

Potential Security Breaches: Potential security breaches involve unauthorized access, disclosure, or manipulation of sensitive data, systems or networks. These breaches can result in significant financial losses, reputational damage and regulatory penalties. Common types of security breaches include data breaches, ransomware attacks, phishing and denial-of-service attacks.

ROI Metric for Design Review Costs vs. Potential Security Breaches

Return on Security Investment (ROSI):

- **Formula:**
  - ROSI=Monetary Value of Risk Reduction−Cost of Design Review
  - Cost of Design Review×100%
  - ROSI=Cost of Design Review Monetary Value of Risk Reduction−Cost of Design Review×100%

- **Monetary Value of Risk Reduction:** The expected financial loss from potential security breaches if design reviews are not conducted.

- **Cost of Design Review:** The total expenses incurred for conducting design reviews, including labor, tools and resources.

Key Metrics to Track

1. **Number of Design Flaws Identified:** The count of potential security issues identified and resolved during design reviews. Higher numbers indicate effective design reviews.
2. **Reduction in Security Incidents:** The decrease in the number of security breaches attributable to design flaws. This metric helps quantify the impact of design reviews on overall security.
3. **Cost Savings from Avoided Breaches:** The financial savings resulting from preventing security breaches through effective design reviews. This includes avoided fines, legal fees and reputational damage.
4. **Compliance Rate:** The percentage of designs that meet regulatory and internal security standards after reviews. Higher compliance rates indicate better alignment with security requirements.

By focusing on these metrics, organizations can effectively measure the ROI of their design review efforts and demonstrate the financial and strategic value of preventing potential security breaches. This approach ensures that all stakeholders understand the importance of thorough design reviews in reducing risk and enhancing profitability.

Reduced Remediation Costs

Definition: Reduced remediation costs refer to the savings achieved by minimizing the expenses associated with fixing security vulnerabilities and breaches. This includes costs for labor, tools and resources required to address security issues.

ROI Metric

Return on Security Investment (ROSI):

- **Formulas:**
  - ROSI=Monetary Value of Risk Reduction−Cost of Remediation / Cost of Remediation×100%
  - ROSI=Cost of Remediation / Monetary Value of Risk Reduction − Cost of Remediation×100%

Key Metrics to Track for Reduced Remediation Costs

1. **Number of Security Incidents**
   - **Reason:** Tracking the number of security incidents helps to measure the effectiveness of remediation efforts. A decrease in incidents indicates that vulnerabilities are being addressed proactively, reducing the need for costly remediation.
2. **Mean Time to Remediate (MTTR)**
   - **Reason:** MTTR measures the average time taken to fix security vulnerabilities. A shorter MTTR suggests efficient remediation processes, leading to lower costs and reduced exposure to risks.
3. **Cost per Incident**
   - **Reason:** This metric calculates the average cost incurred for each security incident. Lower costs per incident indicate more effective and efficient remediation strategies.
4. **Compliance Rate**
   - **Reason:** The percentage of systems that comply with security policies and regulations. Higher compliance rates reduce the likelihood of incidents and the associated remediation costs.
5. **Frequency of Patch Updates**
   - **Reason:** Regular patch updates help prevent vulnerabilities from being exploited. Tracking the frequency of updates ensures that systems are kept secure, reducing the need for remediation.
6. **Reduction in Downtime**
   - **Reason:** Downtime due to security incidents can be costly. Measuring the reduction in downtime as a result of effective remediation efforts highlights the financial benefits of proactive security measures.

Why Focus on These Metrics?

Focusing on these key metrics provides several benefits:

- **Cost Savings:** By tracking and improving these metrics, organizations can significantly reduce the expenses associated with fixing security vulnerabilities and breaches. This leads to substantial cost savings and a higher return on investment (ROI).
- **Improved Security Posture:** Regularly monitoring these metrics helps identify areas for improvement in the organization's security strategy. This proactive approach enhances the overall security posture, reducing the likelihood of incidents and the need for remediation.
- **Regulatory Compliance:** Ensuring high compliance rates with security policies and regulations helps avoid fines and legal issues. This not only saves money but also protects the organization's reputation.
- **Operational Efficiency:** Efficient remediation processes minimize downtime and disruption to business operations. This leads to increased productivity and better resource allocation.
- **Risk Management:** By reducing the number and impact of security incidents, organizations can better manage risks and protect their assets. This proactive risk management approach contributes to long-term stability and growth.

By focusing on these metrics, organizations can effectively measure and improve their remediation efforts, leading to reduced costs, enhanced security, and greater overall efficiency.

Downtime Due to Security Incidents

Downtime Due to Security Incidents: Downtime due to security incidents refers to periods when IT systems, applications or networks are unavailable or non-functional as a result of cyber-attacks, system failures or other security-related disruptions. This unavailability impacts users' ability to access essential services, data or functionalities, leading to potential financial losses, reduced productivity and reputational damage.

ROI Metric for Downtime Due to Security Incidents

Return on Security Investment (ROSI):

- **Formulas:**
    - $\text{ROSI}=\text{Monetary Value of Downtime Reduction}-\text{Cost of Security Investment} / \text{Cost of Security Investment}\times 100\%$
    - $\text{ROSI}=\text{Cost of Security Investment} / \text{Monetary Value of Downtime Reduction}-\text{Cost of Security Investment}\times 100\%$

- **Monetary Value of Downtime Reduction:** The expected financial loss from downtime if no security measures were implemented.

- **Cost of Security Investment:** The total amount spent on security measures to prevent or mitigate downtime.

Key Metrics to Track

1. **Mean Time to Detect (MTTD):** The average time taken to identify a security threat after it has occurred. A lower MTTD indicates more efficient detection capabilities.
2. **Mean Time to Respond (MTTR):** The average time taken to respond to and mitigate a security incident after detection. A lower MTTR reduces the duration of downtime.
3. **Incident Frequency:** The number of security incidents occurring within a specific timeframe. Fewer incidents suggest better overall security posture.
4. **Financial Impact of Downtime:** The total financial losses incurred due to downtime, including lost revenue, productivity and recovery costs.
5. **System Availability:** The percentage of time that IT systems, applications or networks are operational and accessible. Higher availability indicates fewer disruptions and better resilience.

By focusing on these metrics, organizations can effectively measure the ROI of their efforts to reduce downtime due to security incidents. This approach ensures that all stakeholders understand the financial and operational benefits of investing in robust security measures.

Incident Response Costs

Definition: Incident response costs encompass the expenses incurred during the detection, containment, and recovery from security incidents. This includes costs for incident response teams, forensic analysis, and system restoration.

ROI Metric

- **Cost-Benefit Analysis (CBA)**
  - Formulas:
    - CBA = Total Benefits / Total Costs
    - CBA =Total Costs / Total Benefits

- **Example:** If incident response efforts prevent $1 million in losses and cost $250,000, the CBA would be:
  - CBA=1,000,000/250,000=4
  - CBA=250,000/1,000,000=4

Cost of Security Training

Definition: The cost of security training includes expenses related to educating employees on cybersecurity best practices, such as training programs, materials, and time spent on training.

ROI Metric

- **Return on Security Investment (ROSI):**
  - Formulas:
    - ROSI=Monetary Value of Risk Reduction−Cost of Training / Cost of Training×100%
    - ROSI=Cost of Training / Monetary Value of Risk Reduction−Cost of Training×100%

Key Metrics to Track

1. **Mean Time to Detect (MTTD)**
   - **Reason:** MTTD measures the average time taken to identify a security threat after it has occurred. A lower MTTD indicates efficient detection capabilities, reducing the window of opportunity for attackers to cause damage.
2. **Mean Time to Respond (MTTR)**
   - **Reason:** MTTR measures the time taken from detecting an incident to initiating a response. A shorter MTTR minimizes the impact of security incidents, reducing potential financial and operational losses.
3. **Incident Frequency**
   - **Reason:** Tracking the number of security incidents over time helps identify trends and the effectiveness of incident response strategies. A decrease in incident frequency suggests improved security measures and response capabilities.
4. **Cost per Incident**
   - **Reason:** This metric calculates the average cost incurred for each security incident, including labor, tools and resources. Lower costs per incident indicate more efficient and cost-effective incident response processes.
5. **Total Incident Response Costs**
   - **Reason:** Monitoring the total costs associated with incident response, including detection, containment, eradication, and recovery, provides a comprehensive view of the financial impact of security incidents.
6. **Downtime Duration**
   - **Reason:** Measuring the duration of downtime caused by security incidents helps quantify the impact on business operations. Reducing downtime duration minimizes productivity losses and enhances business continuity.
7. **Compliance Rate**
   - **Reason:** The percentage of incidents that are managed in accordance with regulatory and internal security policies. Higher compliance rates indicate effective incident response processes and reduced risk of regulatory penalties.

By focusing on these metrics, organizations can effectively measure and improve their incident response efforts, leading to reduced costs, enhanced security, and greater overall efficiency.

Incident Prevention and Faster Recovery

Definition: Incident prevention and faster recovery involve measures taken to prevent security incidents and reduce the time required to recover from them. This includes proactive security measures and efficient incident response plans.

ROI Metric

Return on Security Investment (ROSI):

- Formulas:
    - ROSI=Monetary Value of Downtime Reduction−Cost of Prevention and Recovery / Cost of Prevention and Recovery×100%
    - ROSI=Cost of Prevention and Recovery / Monetary Value of Downtime Reduction−Cost of Prevention and Recovery×100%

Key Metrics to Track

1. **Mean Time to Detect (MTTD)**
    - **Reason:** MTTD measures the average time taken to identify a security threat after it has occurred. A lower MTTD indicates efficient detection capabilities, reducing the window of opportunity for attackers to cause damage.
2. **Mean Time to Respond (MTTR)**
    - **Reason:** MTTR measures the time taken from detecting an incident to initiating a response. A shorter MTTR minimizes the impact of security incidents, reducing potential financial and operational losses.
3. **Incident Frequency**
    - **Reason:** Tracking the number of security incidents over time helps identify trends and the effectiveness of preventive measures. A decrease in incident frequency suggests improved security measures and response capabilities.
4. **Downtime Duration**
    - **Reason:** Measuring the duration of downtime caused by security incidents helps to quantify the impact on business operations. Reducing downtime duration minimizes productivity losses and enhances business continuity.
5. **Cost per Incident**
    - **Reason:** This metric calculates the average cost incurred for each security incident, including labor, tools and resources. Lower costs per incident indicate more efficient and cost-effective incident response processes.
6. **Compliance Rate**
    - **Reason:** The percentage of incidents that are managed in accordance with regulatory and internal security policies. Higher compliance rates indicate effective incident response processes and reduced risk of regulatory penalties.

By focusing on these metrics, organizations can effectively measure the ROI of their efforts in incident prevention and faster recovery. This approach ensures that all stakeholders understand the financial and operational benefits of investing in robust security measures.

Creating Code - Fewer Vulnerabilities

Definition: Creating code with fewer vulnerabilities involves implementing secure coding practices to minimize security flaws in software development. This includes using best practices, techniques and tools to identify and address potential security issues early in the development lifecycle. Secure coding aims to prevent vulnerabilities such as SQL injection, buffer overflows and cross-site scripting, thereby enhancing the overall security and resilience of the software.

ROI Metric

Return on Security Investment (ROSI):

- Formulas:
  - ROSI=Monetary Value of Risk Reduction−Cost of Secure Coding Practices / Cost of Secure Coding Practices×100%
  - ROSI=Cost of Secure Coding Practices / Monetary Value of Risk Reduction−Cost of Secure Coding Practices×100%

Key Metrics to Track

1. **Number of Vulnerabilities Detected**
   - **Reason:** Tracking the number of vulnerabilities detected during code reviews and testing helps measure the effectiveness of secure coding practices. A decrease in detected vulnerabilities indicates improved code quality and security.
2. **Cost of Fixing Vulnerabilities**
   - **Reason:** This metric calculates the average cost of fixing vulnerabilities identified during development versus post-deployment. Lower costs indicate that vulnerabilities are being addressed earlier in the development process, reducing remediation expenses.
3. **Frequency of Security Audits**
   - **Reason:** Regular security audits help ensure that secure coding practices are being followed consistently. Increased frequency and thoroughness of audits can lead to early detection and mitigation of potential security issues.
4. **Compliance Rate**
   - **Reason:** The percentage of code that complies with secure coding standards and guidelines. Higher compliance rates indicate better adherence to security best practices, reducing the likelihood of vulnerabilities.
5. **Time to Remediate Vulnerabilities**
   - **Reason:** Measuring the time taken to fix identified vulnerabilities helps assess the efficiency of the remediation process. Shorter remediation times indicate a more proactive approach to addressing security issues.

By focusing on these metrics, organizations can effectively measure the ROI of their secure coding efforts, and demonstrate the financial and strategic value of creating code with fewer vulnerabilities. This approach ensures that all stakeholders understand the importance of secure coding in reducing risk and enhancing profitability.

Vulnerabilities Linked to Old Systems

Definition: Vulnerabilities linked to old systems refer to security weaknesses in outdated software and hardware that can be exploited by cyber attackers. These vulnerabilities arise because older systems often lack the latest security updates and patches, making them easier targets for cyber threats. Common risks associated with outdated systems include ransomware, data breaches, malware infections and operational disruptions.

ROI Metric

Return on Security Investment (ROSI):

- Formulas:
  - ROSI=Monetary Value of Risk Reduction−Cost of Upgrading Systems/Cost of Upgrading Systems×100%
  - ROSI=Cost of Upgrading Systems/Monetary Value of Risk Reduction−Cost of Upgrading Systems×100%

Key Metrics to Track

1. **Number of Vulnerabilities Detected**
   - **Reason:** Tracking the number of vulnerabilities identified in old systems helps measure the effectiveness of the upgrade process. A decrease in detected vulnerabilities indicates improved security.
2. **Frequency of Security Incidents**
   - **Reason:** Monitoring the frequency of security incidents related to outdated systems helps assess the impact of upgrades. Fewer incidents suggest better protection and reduced risk.
3. **Cost of Remediation**
   - **Reason:** Calculating the average cost of remediating vulnerabilities in old systems versus upgraded systems helps quantify the financial benefits of the upgrade.
4. **System Downtime**
   - **Reason:** Measuring the duration of downtime caused by vulnerabilities in old systems helps quantify the operational impact. Reduced downtime indicates improved system reliability and availability.
5. **Compliance Rate**
   - **Reason:** The percentage of systems that comply with current security standards and regulations. Higher compliance rates indicate better alignment with security requirements and reduced risk of regulatory penalties.

By focusing on these metrics, organizations can effectively measure the ROI of upgrading old systems and demonstrate the financial and strategic value of reducing vulnerabilities. This approach ensures that all stakeholders understand the importance of maintaining up-to-date systems to enhance security and profitability.

Key Point: Many, if not all, of the above metrics are already being tracked to assess the capability and effectiveness of a cybersecurity program. The next step is to use this information to quantify the risk the organization faces after addressing or neglecting cybersecurity debt. This approach provides the leverage and data needed to have deeper conversations about the intrinsic value of cybersecurity to the organization's bottom line, transforming it into a true enabler of business goals and outcomes.

FINAL THOUGHTS

JOHANN BALAGUER

A key lesson learned from this report is that addressing cybersecurity debt requires a practical, risk-based approach that focuses on critical assets and prioritizing investments to mitigate the risks effectively.

ALICIA CLARKE

I found great value in Bob Turner's "Return on Investment," where the discussion of proactive versus reactive measures is critical and has a significant financial impact. Investing in security measures from the start reduces costs and risk exposure when implemented and configured according to standards. The long-term cost of a breach outweighs the cost of investing in tools, people and processes to prevent a potential disaster.

NIKK GILBERT

From my perspective, the value of this report lies in its ability to bridge the gap between security and business priorities. Cybersecurity debt isn't just about outdated technology—it's about risk trade-offs, leadership decisions and organizational accountability. One key takeaway for me is that addressing cybersecurity debt requires continuous engagement with executive leadership. If CISOs can clearly articulate the cost-benefit relationship of security investments, they will be better positioned to drive meaningful change rather than just firefighting issues as they arise.

MONIQUE HART

Although technical debt is something that we may always struggle with, the report outlined several techniques that can be utilized to help improve one's status and program. There were several metric examples and supporting graphics that could also be used to help a team justify their need but more importantly, allow the business (leadership team and/or board) to understand and support the budget necessary to implement change. Other techniques provided examples for communicating ROI and business justification.

DAVID LACKEY

This collaborative effort is a powerful reminder of why CISO collaboration is essential in addressing complex cybersecurity challenges. Each contributor brought unique insights shaped by their own experiences, highlighting how cybersecurity challenges vary across industries but share common themes. By working together, we gain a broader perspective, uncover new approaches, and strengthen our collective ability to manage risk. No single organization or leader has all the answers, but through open dialogue and shared expertise, we can better navigate the evolving cybersecurity landscape. The discussions that shaped this article reinforce the value of peer collaboration in staying ahead of evolving threats. As CISOs, we must continue fostering these conversations, learning from each other, and strengthening the security community as a whole.

FINAL THOUGHTS

LOCK LANGDON

I found Bob Turner and David Cass' "How Do We Break the Cycle" section incredibly relevant to my own experience juggling security priorities with day-to-day business pressures. They really highlight how unresolved risks and leadership inertia don't just open up security gaps, they also chip away at resilience and stall innovation. Making the right investments in security and building a supportive culture are the only ways to avoid constantly putting out fires and, instead, start preventing them. It's clear that ignoring these issues in the long run will always cost more than addressing them upfront.

BRIAN MILLER

Technical debt is ultimately a problem that has hidden cost and impact on the business of an organization. The more debt you have, the greater drag on an organization and risk to the business. Cybersecurity technical debt is no different than any other kind of IT technical debt. It is important that there is an organizational approach to manage and reduce technical debt on an ongoing basis.

NEDA PITT

In my exploration of cybersecurity debt, you've learned that it represents the accumulation of security vulnerabilities due to rapid digital transformation. CISOs are grappling with the challenge of managing this debt while continuing to innovate. Establishing a clear framework for quantifiable risk discussions with leadership is crucial to align on risk appetite and make informed decisions. As digital transformation is an ongoing journey, so is the mitigation of cybersecurity debt, requiring continuous effort and collaboration. Ensuring all stakeholders have the right information is imperative to reducing and eventually eliminating cybersecurity debt.

HUSSEIN SYED

My peers have provided insights into identifying and addressing security debt. Unmanaged security can lead to operational crisis for an organization. Cybersecurity debt management should be a strategic priority for an organization, utilizing some or all of the approaches in this report. David Lackey's insights in "The Unseen Consequences of Digital Transformation," and Bob Turner and David Cass's section on "How Do We Break the Cycle" combined present a case for management to put emphasis on this critical risk.

BOB TURNER

I found great value in David Lackey's section titled "The Unseen Consequence of Digital Transformation," where he identified how teams become overwhelmed by the multi-threaded tasks of building and maintaining infrastructure while deploying new technologies. How do architects and engineers pursue competing efforts to "keep the lights on" while trying to innovate and accelerate deployment? How should technologists respond to critical system development and deployment issues alongside leadership pressures? Specifically, those pressures cause a loss of focus on the competing actions of maintaining the system, optimization of the resources, and the challenge of keeping up with security related failures.

nagomi

Nagomi automates the process of proving your security is actually working. Our platform unifies data across your assets, defenses, and threats to clearly illustrate your security program is both efficient and effective to key stakeholders. This transparency helps you demonstrate measurable results with confidence. By maximizing existing investments, reducing threat exposure, and improving alignment across teams, Nagomi is the only Proactive Defense Platform that turns cybersecurity from a technical cost center into a strategic business enabler. With Nagomi, security goes from feeling fragmented and overwhelming to streamlined and effective—leveraging the tools you already have.

CISO INCLUSIONS

We asked our CISO contributors to share their thoughts on this important topic. What follows are their challenges and opportunities to reduce cybersecurity debt.

Disclaimer: The views expressed in this report are solely those of the authors based on their experiences in the CISO role.

JOHANN BALAGUER

Chief Information Security Officer, Hard Rock

Cybersecurity debt can cause significant organizational issues if not properly managed. Effective posture management, understanding and prioritization are essential to address it. Although addressing cybersecurity debt is costly, some investment is unavoidable. Organizations need to make risk-based decisions, focusing on critical assets like revenue-generating and essential operational systems. They assess whether issues require immediate action or if they can be mitigated through controls.

Debt Dashboard

Tracking cybersecurity debt over time with a dashboard helps monitor active efforts and alerts the team to upcoming end-of-life systems, allowing for budget planning in advance.

Process debt, another form of cybersecurity debt, requires funding and resources to improve capabilities if processes are ineffective.

Complete visibility of cybersecurity debt can be achieved using asset posture management technologies and third party tools. Once identified, security debt can be categorized by risk level to determine urgent investments and potential decommissioning.

Teams can assess the financial and operational impact of cybersecurity debt through calculations using cyber risk quantification models like Factor Analysis of Information Risk (FAIR™) to evaluate risks based on data.

Industry Specific

All organizations have cybersecurity debt, but different industries address it in different ways. An organizational risk committee or other risk management function is the starting point for discussions about assets, posture, and the amount of technical and cybersecurity debt an organization has.

No organization has an unlimited budget, so investments must be prioritized. Strong data points are essential to help leaders decide between remediations or funding innovation and customer enhancements. Will the costs outweigh the potential revenue from improved customer experience? This challenging decision requires solid data to make well-informed decisions.

Displaying KPIs and showcasing cybersecurity maturity effectively demonstrates ROI. The use of KPIs and metrics over time shows how investments have strengthened areas of your security or vulnerability management programs.

Budgets to address cybersecurity debt are increasing as organizations continue to observe daily breaches and attacks in the news. It is recognized that an organization can be significantly impacted if these weaknesses are exploited by malicious threat actors. There is a responsibility to mitigate these issues, and executives and boards are providing the support that is needed.

DAVID CASS

Chief Information Security Officer, GSR

All organizations have cybersecurity debt to some extent. Your tech stack profile will determine how easy or challenging it will be to resolve. But it is definitely something that all organizations have to deal with.

Failure to deal with cybersecurity debt means systems will evolve to a point where they can no longer be monitored effectively. Tools will become incompatible with the newer tech stack, with an array of potential implications including reduced visibility; monitoring failures; and audit and credentialing problems deriving from the inability to integrate with cloud and SaaS platforms.

All organizations must do risk assessments, and debt should be included in those calculations to understand its potential impact. That way you can focus on addressing the higher risks first, and plan a roadmap.

Organizations, especially if they're regulated, are expected to have that discipline. But a surprising number of regulated companies still get caught holding the bag because they fail to realize how much planning is actually required when end of life and end of service looms. By the time they hit, the company is probably losing money because it is paying vendors for extended support, and a huge exposure is created.

Education Overlooked

Education and training for the team is often overlooked when considering cybersecurity debt. As new technology comes online, it is critical that the development , operations and security teams understand it, and the best practices for securing it. It's one thing to spend a fixed amount on a fancy new tool, but if you have nobody to operate it, it has no value. Organizations must understand the need to invest to upskill teams to get the real benefit of new technology.

Dealing with cybersecurity debt is easier when a company is cloud- and SaaS based. Updates will appear in configuration management on a regular basis, and they are highly automatable. Most big cloud service providers will force customers to upgrade their platforms by automatically updating them if clients get too far behind in their revisions. It's not advisable to be automatically updated, however, because in most cases, you want to evaluate the generations or revisions to make sure everything is compatible.

Burden Shift

As organizations move to cloud and SaaS, there will be a shifting of the cybersecurity debt burden. Obsolescence now becomes the responsibility of the vendor or cloud provider. It's obviously in their best interest to keep things up to date, because a major hack at a cloud service provider or a major SaaS platform would have a ripple effect. So rather than have the cybersecurity debt burden on the CISO to budget consistently for upgrades, automatic updates become part of the cloud or SaaS pricing plan.

Industries with large technical portfolios, like big tech or big banks, have significant cybersecurity and tech debt, so migration to the cloud and SaaS requires a great deal of planning. Many early cloud adopters just took their legacy tech stacks and tucked them into the cloud, and that did not turn out well. That "lift-and-shift" practice didn't allow these companies to reap the real benefits from the cloud, such as microservices and diverse data structures, and required the addition of a new team just to deal with the new architecture.

Larger companies therefore need to be very thoughtful on how they approach migration into the cloud or SaaS. The optimal strategy is to migrate areas that either pose the greatest risk, because they're end of life or end of service, or areas where the business can benefit most from cloud or SaaS.

DAVID CASS

Chief Information Security Officer, GSR

Extensible Tools

Make sure tools are extensible and can take advantage of the cloud. A major component is getting security practices embedded into the CI/CD pipeline when migrating. Strive to find tools that can be used across multiple products so they don't necessarily become obsolete.

At the same time, if the business suddenly decides it needs to add multiple new SaaS products, it is faster to switch security tools because they're cloud based. Retooling isn't nearly as painful as trying to redo an entire enterprise system, which could take many months of planning and coordination among teams.

During our regular security and risk assessments, we look out our own tech stack to determine whether products are still fit for the purpose. That could mean end of life or end of service. But because cloud and SaaS technology changes so often, it could also mean finding new products that have more capability than you currently have.

We still have to budget, but it's more on the basis of capacity planning and feature and functionality upgrades versus product obsolescence.

Measuring Cost

Measuring the cost of cybersecurity debt to the company can be quite tricky because many organizations consider it as a tax that each business unit pays. Cloud affords a better metering capability. Because it allows a high diversity of services, high-risk business units can be charged for additional services they need, versus a one-size-fits-all model.

Most organizations lump their technical debt all in one space, which can make it hard to factor out actual security costs. When security chiefs control their own budgets, they can allocate as they need. Budgets coming out of the CTO or the CIO might have competing priorities that might make it more challenging.

ROI is a challenging way to justify debt alleviation because security is like a utility: Nobody really knows it's there until the lights go out. Try, therefore, to figure out what resonates with the business.

I try to tie new capabilities to meeting the many regulatory requirements the financial services sector has, because that makes it much easier to justify the need. Return on investment can also be justified by explaining how the new investment would reduce risk to the organization. It's more a matter of how much risk is being reduced, and quantifying that risk, rather than creating a pure ROI model.

ALICIA CLARKE

Head of Cybersecurity, PGA TOUR Superstore

In today's rapidly evolving digital landscape, managing cybersecurity debt is crucial, even for small- to mid-size businesses like us. While our reliance on SaaS solutions minimizes our data center footprint, my previous experience with mergers and acquisitions highlighted the challenges of integrating outdated platforms and the loss of institutional knowledge. To mitigate these risks, we implemented controls to protect legacy applications, accepting the inherent risks involved.

Vulnerability Scans

Our approach to identifying system flaws involves both static and dynamic vulnerability scans. Critical systems are monitored by agents that scan throughout the day, supplemented by monthly scans. The results are reported regularly to management, ensuring timely remediation based on compliance requirements and the severity of the issues.

We leverage third-party services for deeper penetration tests, vulnerability assessments and continuous network and application scans. These services provide insights into vulnerabilities and prioritize remediation efforts. Additionally, we use external threat intelligence tools to monitor for brand impersonation and compromised employee email addresses on the dark web.

Leadership and Risk Assessment

Educating leadership about risks, such as outdated systems, is essential. As a leader, I present potential financial impacts and propose solutions or mitigations. This proactive approach fosters informed decision-making and prioritization of security initiatives.

When advocating for investments, I lead with compliance requirements to underscore the necessity. Sometimes, I bring in third-party experts to provide additional context and support. This strategy helps business leaders understand the importance of the investment and its impact on our operations.

Negotiating with vendors requires creativity. I seek affiliations that allow us to capitalize on tools and find solutions that address multiple needs. This approach maximizes ROI and enhances organizational productivity by enabling employees to focus on priority tasks.

Cyber Insurance

Cyber insurance is a critical consideration in managing security debt. Ensuring accurate responses to insurance questionnaires and implementing robust controls are vital to securing coverage. As the landscape evolves, insurers may demand more direct verification of our security measures.

Data privacy is mission critical. Good privacy is good business, Business leaders must recognize the value of investing in the right tools and leadership to sustain long-term success. From regulation to reputation, compromising data privacy is not worth the risk.

NIKK GILBERT

Chief Information Security Officer, RWE

Defining Cybersecurity Debt

I use the term “cybersecurity debt” to describe any neglected or overlooked weaknesses in an organization’s security posture. These are issues that, for various reasons, never rose to a high enough priority level to get fixed. Large enterprises often face more significant challenges elsewhere, causing smaller or remote systems to slip through the cracks. Unfortunately, those overlooked systems can be exactly what malicious actors seek out.

It is not realistic to eradicate every single security risk. The most crucial step is to assess your cybersecurity debt and then tackle it piece by piece with a practical, risk-based approach. That is the message your board needs to understand: there is no such thing as zero risk, and sometimes bad things happen to good organizations.

Risk Rank Your Debt

After nearly three decades as a CISO, I have found the best way to begin addressing cybersecurity debt is by determining which risks pose the greatest threat. Know your organization’s “crown jewels,” focus on those first, and develop a formal plan, notably a well- practiced incident response plan. This way, if an incident does occur, the team can respond quickly and effectively, minimizing loss and downtime.

Legacy technology is a significant contributor to cybersecurity debt. Eliminating or upgrading these older systems can be expensive and complicated. Vendors might be reluctant to update products because of narrow profit margins or resource constraints. In those cases, accepting the risk may be the only viable path, which makes a robust incident response plan even more critical.

Securing Executive Buy-In

When I joined my current organization, I evaluated our security posture against a well-known industry framework and proposed aiming slightly above the benchmark. By articulating both the need and the strategy, along with the required resources, senior leadership understood precisely what it would take to elevate our defenses, and they supported it.

This underscores the second essential element of handling cybersecurity debt: effective communication. Technical jargon can undermine trust and engagement. Instead, frame security concerns in terms of business impact and risk management. A one-page cybersecurity strategy conveying how you will thwart potential threats in plain language often resonates far better than a dense technical document.

Building Trust and Advocacy

To get organizational buy-in, focus on how you can solve real problems for people. Making employees’ lives easier, whether by improving user experiences or streamlining processes, helps illustrate the value of proactive security measures. Once teams see tangible benefits, they are more likely to support security initiatives.

Sometimes, you will find allies who naturally share your vision, but other times, you have to bring people around. Either way, the more advocates you build, the more effectively you can address and reduce cybersecurity debt.

MONIQUE HART

Vice President of Information Security, Healthcare Industry

Given the use of technology today, few security leaders will feel as though they have the resources (people and/or technology) necessary to fully eliminate security debt in their environment. And this couldn't be truer than in the healthcare space, where technology that is used to help treat patients is built to last for years and well past systems support and end of life agreements. This can slow down our ability to function and protect our organizations in a way that everyone hopes they are being protected, especially if compounded with experienced resources debt. But the biggest debt I see is when a CISO can't tie how information security or cybersecurity benefits the organization's mission.

Unless the business understands how information security contributes to the organization's mission, there will be little to no buy-in. It is not an effective strategy to talk only about what attackers can do and how critical a certain technology might be at that time. But we have to be able to translate the technical concerns into relatable stories as well as justify why such technology and people are needed to support the environment and their positive ROI. I have gotten buy-in through storytelling that shows how security is a part of patient safety, which is our supreme mission. In health care, the wrong analysis can affect a person's life.

High Priority

It was made very clear to me when I started nine years ago at my current organization that security debt was one of the top three areas of importance. Leadership had been focusing on recently reported ransomware attacks and the impact to other healthcare organizations. They had an outside firm complete an assessment on their security posture prior to my onboarding. I was asked to review the analysis and build a program based on the facts presented and my experience of building programs elsewhere.

When I started, we had three people and one solution to focus on five hospitals. The priority was vulnerability scanning and meeting compliance. I used the information provided to help identify the resources and technology needed to expand the focus to include areas such as incident response, forensic analysis, security architecture, medical device security, risk management, policy governance, and user training and awareness.

Hence, the group has grown exponentially since that time but so has the organization: Today we are the largest healthcare system across our state. And we have brought on many different groups with different systems for patient care. So security debt is something we think about daily.

Compounded Debt

When a hospital or practice is acquired, the security debt is compounded. And because we've grown, it is challenging to identify the exact number of resources we need. We have to assess what technologies we are bringing on board and where we quickly have to make changes to reduce our risks. Those risks exist both in terms of connecting the new business to our network, ensuring that individuals coming on board are familiar with our practices and policies, and know how to manage our systems without causing risk. It's also important to know when a vulnerability cannot be eliminated but must be contained in order to continue using the system and have assurances that it is functioning as expected without compromising the environment or patient data.

It can be challenging to identify the exact number of resources needed to keep things flowing efficiently, especially during M&amp;A growth. A key piece of security debt is remembering the human behind all these elements, and taking the time to perform due diligence so they don't burn out. You want to create an environment that promotes very little turnover.

MONIQUE HART

Vice President of Information Security, Healthcare Industry

Optimally you have assessors to help you analyze what processes can be improved or which technologies can improve the processes to help reduce your resources' workload. It can also help when you have a third party come in to help share your story to leadership. But most important, have empathy and listen to your people's concerns: Acknowledge the work necessary to address the vast changes in the technology and attack landscapes that have happened in the last few years.

Education is another big component of alleviating security debt. It's crucial that my team has the time to train on what's happening in the world, and that we have the capability to keep up with what's going on. If you're knee deep in trying to resolve all the issues in front of you, and time is not allotted for education on what could happen, they will constantly be playing catchup and it will only make matters worse. And security education can't be limited to the security team: Security is everybody's business. It must encompass changes in technologies so various teams can properly understand, deploy and support these solutions.

Calculating Debt

We have several forms of KPI to calculate security debt, ranging from how many requests our employees are managing, to what technologies we have and their ability to perform the functions we need to protect the environment. What we have learned from recent upgrades during the mergers is that there is a tendency for redundancy and insufficiency. Every year we go through the process of identifying and assessing all of the solutions we have, and how they are best supporting what we are seeing. We also review whether our people have the right skillsets to support the changes and technologies, or if education and more staff is needed.

Before any new technology is brought into the organization, we go through a security risk assessment that reviews the technology's capabilities, how the solution needs to be configured in our environment, and the vendor's security practices.

In the information security space, we focus a lot on the risk component of the business analysis. One of our most important KPIs is inherent risk versus residual risk, because it's an important metric to show how we improved our security posture and possibly avoided a patient-impacting incident. It's one thing to find vulnerabilities, but we also need to know whether they have been addressed.

Vulnerabilities Down

Our last quarterly assessment showed that we were able to reduce high and critical vulnerabilities from 38% to less than 2%. These assessments allow the organization to see what we're adopting and how we've been able to reduce risk, including avoiding or lessening the impact from third-party crises such as the MOVEit and Change Healthcare breaches.

When discussing the financial and operational impact of security debt, I usually ask those leaders to monetize the cost to the organization if patients can't access our website or use our payment portal. And while I can't put a monetary value on our reputation, I can point to penalties that similar organizations have had to pay for HIPAA violations.

Budget is always tight in healthcare, but especially in a nonprofit organization. What I really appreciate about my organization today is that although we have a set budget, they understand the need and have set up a contingency fund. As long as you can justify and truly show the need, the conversation isn't closed, and there is a way to work with leadership, and even our vendors, to help us address the issues we have.

DAVID LACKEY

Chief Information Security Officer, World Vision

As organizations embark on or complete their digital transformation journey, they often find themselves burdened with an unanticipated form of cybersecurity debt. This debt arises from failing to recognize and address the profound cybersecurity challenges of a digitally transformed world, where data, services and workforces are decentralized and highly distributed.

In this new paradigm, traditional security tools and approaches that once sufficed for centralized, on-premises environments are proving inadequate. Legacy solutions often lack the scalability and flexibility required to secure modern SaaS applications, cloud-native architectures and interconnected systems. The result is a patchwork of tools and processes that struggle to provide comprehensive visibility, governance and control across a sprawling digital ecosystem.

Security Implications

Organizations commonly do not understand the implications of going through a digital transformation from a cybersecurity perspective. They fail to recognize that effective cybersecurity in a digitally transformed world requires a fundamental shift in strategy, and not just incremental adjustments. They need to adopt tools and frameworks specifically designed for dynamic, decentralized environments, and build governance models that align with the new reality of digital business operations.

Without a shift in strategy, organizations risk compounding their cybersecurity debt, leaving themselves vulnerable to emerging threats and regulatory scrutiny. Addressing this challenge requires proactive investments in scalable security solutions, enhanced governance practices, and a commitment to aligning cybersecurity strategy with the operational realities of a digitally transformed enterprise.

When a company plans to undergo digital transformation, security leaders need to become part of the conversation early on. They need to explain the cybersecurity consequences and the governance-risk-compliance implications, and have a vision and a strategy that is tied to the objectives of the organization. That will aid in prioritization while pushing for budgets to keep the organization secure.

Neglected Best Practices

Another critical contributor to the accumulation of cybersecurity debt lies in the neglect of configuration best practices. In their eagerness to innovate and deploy new capabilities, many organizations lose sight of the foundational elements of cybersecurity hygiene. This oversight often stems from a hyper-focus on rapid implementation, leaving configurations incomplete, inconsistent or misaligned with industry standards.

Compounding this issue is the dual role of operations and engineering teams in many organizations. These teams are tasked with both building and maintaining infrastructure and deploying new technologies. As a result, their focus frequently shifts to the demands of innovation and deployment, causing them to overlook the maintenance and optimization of tools and technologies already in use. This creates a cascading effect, where outdated configurations and neglected security tools further deepen the organization’s cybersecurity debt.

Back to Basics

I have implemented a shared annual initiative across all teams called "Back to Basics." This program ensures that configuration reviews of technology and security tools are a formalized goal each year. We test our security tools through different types of exercises to make sure they are configured to a specific standard and that they are actually effective. We also make sure that every person, every process and every tool has a plan.

LOCK LANGDON

Chief Information Security Officer, Aprio

The goal is to realign with best practices, optimize existing tools, and reduce unnecessary complexity in security operations. By dedicating time and resources to this initiative, organizations can proactively mitigate cybersecurity debt, strengthen their defenses, and lay a robust foundation for future growth.

Neglecting best practices and operational basics may seem inconsequential in the short term, but it can significantly exacerbate vulnerabilities over time. A structured, deliberate focus on revisiting and reinforcing these fundamentals is a vital step in combating the silent accrual of cybersecurity debt.

For me, the number one concern for technology and executive leadership often revolves around unresolved risks—those persistent "gremlins in the closet"—that remain due to limited authority, budget, or staffing.

Over the past five years, our company has expanded nearly tenfold to almost 3,000 employees, a significant portion through mergers and acquisitions (M&As). This rapid growth has resulted in significant technical debt, much of it legacy-based or inherited through acquisitions. Our strategy focuses on mitigating identified technical and cybersecurity debt, removing outdated or risky technologies when possible, and documenting and accepting technical debt where mitigation is not feasible.

Learning the Nuances of M&As

Since mergers and acquisitions have been the main drivers of our company's growth, we must learn the nuances of the new businesses we integrate. As a financial services organization, most of our business is tax-related. However, if we onboard a new federal government auditing group, we must adapt to stringent federal compliance and regulatory requirements within that space.

The tools and technology utilized by new acquisitions often don't align with our enterprise standards. As a maturing organization, we can lack internal expertise to manage unfamiliar tools and technologies. Additionally, when IT services have been outsourced, ending that relationship during the acquisition creates significant organizational knowledge gaps.

A Three-Tier Strategy for Integration

Our approach to onboarding a new company's tech stack follows a three-tier strategy:

1. Replace: Transition to our trusted security stack.
2. Accept: Retain the acquired company's tech stack and manage the associated technical debt.
3. Adopt: Incorporate the acquired tech stack as a new enterprise standard.
4. Recruiting expertise

To assess the technical debt of acquired companies, we sometimes use internal tools but often rely on trusted third-party experts. For example, during a merger with a FinTech company, we recruited external specialists to conduct a detailed development discovery process. These experts ensured we fully understood the complexities of their software development operations. Executive leadership support is crucial for securing the financial resources to make such evaluations part of the M&A playbook.

Playing Offense: Threat Intelligence

Proactive security measures leverage tools that deliver threat intelligence concerning potential acquisition targets. These tools evaluate risks within a company, pinpoint vulnerabilities, and document their findings. Additionally, they offer insights into known risks or threats in the environment, functioning as an intelligence platform.

LOCK LANGDON

Chief Information Security Officer, Aprio

In my opinion, the most effective tools are those that automate labor-intensive tasks or reduce false positives. This enables teams to concentrate on actionable insights and remediation rather than just delivering more dashboards showing what is wrong.

Couching Risk in Business Terms

From business leaders' perspectives, M&As represent opportunities for financial growth. As a CISO, I am responsible for articulating the risks associated with these opportunities and establishing a secure plan for integration.

Maintaining an accurate inventory of assets, networks, applications, and tools is foundational to identifying and managing technical debt. Without this baseline, understanding the scope of security challenges becomes impossible.

Measuring the Impact of Security Debt

We leverage the Factor Analysis of Information Risk (FAIR™) framework to quantify and document risks in financial terms. While FAIR™ focuses on risk rather than debt, it provides a clear picture of potential exposure. Other resources, such as the Verizon Data Breach Investigations Report, also help estimate vulnerabilities' financial and operational impact.

Framing risks in dollar terms greatly benefits budget discussions. Effective prioritization is key, as resources are always limited. Balancing newly identified vulnerabilities with previously documented ones requires constant effort and strategic juggling.

Competing Assessments and Risk Acceptance

If a risk is articulated and its impact documented, yet the business decides it is not a priority, this acts as a "pressure relief valve" for the CISO. The SEC and other regulatory agencies generally accept such decisions as long as the risk has been transparently communicated and formally accepted.

What is Unacceptable is Undocumented or Hidden Risk

To ensure clarity and accountability, we maintain a Risk Council of executive leaders that meets monthly to review and address active risks. For high-priority issues, we consult the CEO and the board to decide on mitigation, acceptance, or budget allocation. A robust Governance Risk and Compliance (GRC) process is essential for documenting and communicating risks effectively. Whether you use a simple spreadsheet or an enterprise-grade GRC platform, the best tool is the one you use.

Mental Well-Being and the Weight of Responsibility

As a CISO, the weight of responsibility often feels immense. Stress arises when we manage issues beyond our authority or resources, leading to frustration and helplessness. Understanding the difference between security issues and wider business challenges is crucial. By articulating and communicating this difference, a significant stress point can be mitigated, and you can work as a cohesive team to tackle, or accept the risks in your organization.

BRIAN MILLER

Chief Information Security Officer, Healthfirst

Most hacks are tied to cybersecurity debt, succeeding because of basic things we know to do that aren't properly addressed.

I see narrowing cybersecurity debt as a top priority. As we work through technical debt, our decision-making is based on whether we deem a particular risk to be manageable with compensating controls, allowing us to invest on an ongoing basis to reduce the risk and exposure, or a fire that we need to address as a priority incident. If the IT team decides it's a fire, then we take care of it immediately. This has allowed us to reduce risk related to technical debt while building an "End of Life" program that consistently engages IT and the business to consistently retire old systems and address technical debt.

Technical debt not only creates security risk but also creates operational and business risk in terms of system and business outages caused by old systems and processes. When it comes to communicating the cost of technical debt, I don't use ROI models that tend to get very technical. Instead, I prefer to identify the things that can disrupt or impact the business, and communicate the cost of not doing things. Ultimately security is about securing the business and its members/customers. During my nearly 10 years at Healthfirst, my mantra has been, "it's all about the business."

Risk Snapshot

As a part of identifying risk, to include technical debt, we do a NIST risk assessment every year. We also do high-trust assessments of all our applications. These assessments give us a picture of where our risk exists both on the program and technical levels. We do ongoing penetration tests and red teaming to test different kinds of attacks to see if they can exploit our known vulnerabilities.

I have found that not every critical vulnerability is likely to be exploited, given our stringent controls. We have gravitated toward using test results and technologies that whittle down the large numbers of the most serious vulnerabilities that organizations typically have to the ones most likely to actually be exploited in order to prioritize. Tools and processes that help us quantify what's really exploitable help us to be more effective at managing risk. This visibility into risks and vulnerabilities also helps us to make sure there are very robust security controls that provide protections where they are needed most.

Biggest Impact

When tackling cybersecurity debt, the best strategy is to identify what will do most to reduce risk and unresolved security vulnerabilities. Go after the big rocks first, such as end-of-life systems that are out of support, then proceed to the many little pebbles that are harder to move, but taken together, constitute a big rock, like secrets and code.

I break cybersecurity debt into three categories -- infrastructure, which includes servers and workstations; the development environment; and identity management.

I started on a server modernization project to identify every server that's going out of support as a first step in seriously addressing enterprise technical debt. Once these were identified, we were able to work with IT and the business to resolve legacy issues and then move to doing a continuous burndown to address systems as they go end of life. As the program matured, we have been able to expand to address more granular technical debt.

BRIAN MILLER

Chief Information Security Officer, Healthfirst

Outdated Systems

I am hearing, though, that a lot of companies still run very old Windows and Linux systems – things that were optimal at the time but now are the wrong solution. These systems remain a challenge either because the right people don't have visibility; because of the complexity that arises from a legacy platform being interwoven into many business processes; and because of the change management and organizational challenges in getting people aligned around a difficult problem that will touch so many organizations and interrupt so many business processes.

Sometimes companies will deliberately hold on to older systems because they need the data for compliance reasons and cannot access it without the old operating system. Those last-mile pieces require changing other systems and a lot of back-end work because they connect across many systems, or have an old piece of software on them that has no newer version that runs on these old operating systems. But optimally the security team would track these systems and set an explicit end date for decommissioning them and finding the optimal path forward.

Heads Up!

With tech debt on servers and infrastructure, it's a good idea to tell people 18 months ahead of time that the work has to be done. During that lead-up, educate the company so that there is an understood risk and an understood process. Once you get that first big chunk of technical debt from servers out of the way, continue the program to keep everything up to date, and clean up any of the more complicated issues that may remain.

With the application development piece, the question is whether things are coded securely and using best practices. If your company doesn't have an application security program, start small. Begin to educate by providing technical solutions to get rid of the security flaws, then make sure the solutions are being coded in. Expand to other applications over time.

Secrets

Another part of appdev security is the "secrets," those privileged credentials that allow access to protected resources, and are authenticated by code. It wasn't until the past 10 years that we had good, viable solutions, so now some companies have technical debt in their code repositories reaching back decades ago when they were founded. These repositories are a good place for hackers to go, so it's advisable to clean them all up. We have a very robust program addressing that.

Privileged identities, both human and non-human, constitute the third circle of technical debt, straddling the other two components by involving both infrastructure security and application security.

The more cybersecurity debt you have, the more your cyber insurance is going to cost. As a CISO, I look at the questions the insurers are asking me about the key
pieces of debt that they think are going to cause a breach. And if I don't have a specific area in hand, I put that as one of my priorities, because I know it's something the insurance company is worried about, so I should be worrying about it, too.

BRIAN MILLER

Chief Information Security Officer, Healthfirst

Budgets Growing

With the multiplicity of breaches and the visibility of the problem, security budgets have been steadily increasing over the past 10 years. The SEC has fueled that growth by holding public boards directly responsible and requiring a very quick disclosure on any material breach.

With virtually all the PHI data stolen through hacks like Equifax or the Change Healthcare hack, new technologies have become a critical part of improving existing systems to protect members and customers. Solutions like LexisNexis iIdentity proofing allow you to fingerprint the device and validate customer data that someone is using as a risk-based way to ensure we are serving our customers while improving our organization's ability to do business.

I see this kind of approach as a good way to leverage existing investments without treating existing investments as technical debt. Sometimes this kind of investment will require a significant increase in budget, but in protecting the core investment in business solutions in a material way, I have found that the cost becomes less of an issue.

That said, the goal is to produce the most value for the least cost for your members or consumers, while at the same time protecting both legacy and new enterprise capabilities.

Process Debt

A lot of the process we do had been very human intensive in the past, and we're automating as much of that as possible. As I brought in more and more automation and artificial intelligence to automate my processes, I've been able to upskill my team to focus on the harder problems that AI can't solve, and to build new processes to support our security work. I have also worked to ensure our security processes mature with our organization. A healthy organization is a growing, evolving organism. To stay on a good trajectory, I work to identify and retire old processes, optimize existing process, and align our process with organizational change and growth.

NEDA PITT

Chief Information Security Officer, Belk

Cybersecurity debt is one of the most significant vulnerabilities undermining a business's ability to build a strong security foundation. The areas where cybersecurity debt accumulates are often the most prone to breaches, making it a critical concern for all organizations.

Many are beginning to recognize the seriousness of this issue, and I foresee a significant shift in the next 12 to 18 months as awareness increases that accumulated technical debt is a key contributor to security debt.

As breaches become more frequent, exacerbated by rapid advancements in AI, security practitioners will face growing challenges in detecting these threats. This will inevitably impact the organization's bottom line, leading to widespread acknowledgment of the problem. At that point, it will no longer be just a concern for the Chief Information Security Officer (CISO) or the information security team; it will require thoroughly examining the organization's infrastructure.

Hindered Modernization

Like many retailers and companies, Belk is navigating the challenges of cybersecurity debt, which has influenced our overall risk posture and slowed our modernization efforts. Addressing this debt has become a priority for us, and we are actively developing roadmaps to tackle it.

Our end-of-life systems, which cannot be patched, require mitigation efforts that divert valuable human resources from more strategic tasks. Therefore, upgrading our systems will ultimately be a significant benefit.

Problems at other organizations heightened awareness among our leadership of the need to address cybersecurity debt. We all know that it is a matter of when, not if, a breach will occur. Although the faulty CrowdStrike update was not related to cybersecurity debt, its reverberation across the globe made leaders think about business continuity planning in more finite terms. But there is only so much that can be done when organizations accept major cybersecurity debt, so the debt needs to shrink.

We are moving over to the cloud as much as we can, and we are having discussions with leadership about long-term aims. It is not just a matter of “moving to the cloud.” We have to decide what needs to be replaced. What is the goal, and how do we get there? How does digital transformation get us to zero trust, reduce our overall risk and increase our overall security posture, while increasing throughput into our system?

ROI and Risk

Ultimately, the conversation is always about return on investment or risk mitigation.

We have begun to use the Factor Analysis of Information Risk (FAIR™) framework to calculate ROI on cybersecurity debt, because it helps us to quantify the actual risk. FAIR™ allows us to calculate the likelihood of an issue and its potential impact, so we can get an actual dollar amount on the costs of cyber attacks. It helps us tell our story and make a compelling argument for investment.

Without a methodology, you are pretty much pulling numbers out of a hat. With FAIR™, I will be able to talk to our CFO and CIO about how much risk we’re holding, how we are mitigating it currently and what it’s costing us, versus how we could modernize and how much risk that would reduce.

At the end of the day, my mandate is to reduce the risk to the organization. If I can save money while doing that, it’s a home run.

NEDA PITT

Chief Information Security Officer, Belk

And Processes

Usually, the majority of risk in an organization comes from technical debt. But it is also imperative to think about process debt, and I have conditioned my team to think about processes. Process must align to changes in the environment, so when we look at our security stack, we also look at it from the process perspective. Where are the bottlenecks? Do we need a new or better technology, or will a process fix make the technology we have work better? We come at it from both sides.

Putting in a shiny new object won't make a problem disappear. There are no silver bullets. When you put in a new system, you also have to build the process and tune that new tool. If you can enhance the process with a tool you currently have, then you have saved the company money while reducing the debt. It's an all-around win.

Insurer Scrutiny

Insurers are scrutinizing security programs harder as attacks multiply. They are digging in to see what organizations are doing to alleviate their technical debt because they understand technical debt leads to security issues that can lead to claims.

Clearly we can't fix everything: Organizations wouldn't be profitable if we did. We must prioritize, and have a plan to fix things to show we understand there is an issue. Insurers are starting to hold organizations accountable for plans to reduce cybersecurity debt, increase their security posture, and ensure they're following accepted security norms and standards.

In the past, people shied from talking about technical debt, but then digital transformation came along and technical debt raised its ugly little head, because you cannot move to the cloud unless you fix certain things. Now the cybersecurity debt that is intrinsic to technical debt is starting to raise its ugly little head. The time has come to treat it like we treated digital transformation.

HUSSEIN SYED

Chief Information Security Officer, RWJ Barnabas Health

Cybersecurity debt, a subset of technology debt, is always a concern for organizations. Many older systems were built with limited security controls compared to the newer systems. Security toolsets and technologies themselves age and become a debt due to their deprecating capabilities against newer and emerging threats.

On the process side, people become used to performing tasks in manners that may become inefficient and time consuming. Change requires re-engineering of the processes, and that requires assessing the current state, identifying threats or risks, developing adaptive processes, testing for efficacy, training the teams, and implementation. Optimization requires collecting relevant metrics to monitor performance and use to improve the processes to attain acceptable maturity.

Organizations make strategic decisions to overcome many of these challenges. In recent years, leading organizations have started to take a stronger position toward technology debt and to support it with newer technology They have formed technology committees to identify obsolete systems and strategize to replace them with newer and better technology, a project termed digital transformation.

High-Ranking Risk

For most organizations, cybersecurity debt is among the top-10 risks. If something is not protected, then it could be compromised. If it's not supported and maintained, then it will break down, causing disruption of services leading to reputational or strategic risk with revenue impact. Executives expect to understand what the organization's strategic plans are around a particular initiative and how their investment will benefit the company; capital investments are allocated based on that.

Progressive organizations want the risk of tech debt to trend down, and be at an acceptable level for areas with a low risk. Budget approvals can be tough, but the scrutiny forces people to demonstrate fiduciary oversight of how they're spending the dollars so people are held accountable.

Driving Change

Technologies such as operational, medical and physical security have a life cycle of up to 20 years. Cybersecurity leaders need to work with business units to articulate the risks and understand how they can operate if they must keep these older technologies in place for longer than we expected to meet business needs.

If organizations don't take strategic approaches to lower or control the cybersecurity debt, potential long-term consequences aren't limited to security risks alone. There is going to be innovation risk as well. Business operations may be impacted as well, with older technology possibly being less precise and more time-consuming and high on carbon footprint. The only option left is to isolate them into a segmented network, but then interoperability becomes a challenge, again raising the risk factor. This can ultimately lead to existential threat.

Dramatic Changes

In the past five years, the security landscape has drastically changed. Things once considered nice to have, like multifactor authentication and encryption, are now considered must have. But a lot of technology in use environments is older because it is expensive, and the redesign of a technology requires quite a bit of work and cost to obtain approvals. But ultimately when risk is not tolerable, a technology has to be replaced with a new technology or some compensating solution. Alternatively, technology has to be implemented to protect it.

HUSSEIN SYED

Chief Information Security Officer, RWJ Barnabas Health

The NIST cybersecurity framework can be used to assess controls, and any technology that cannot meet the control specifications gets added to the risk register, where its severity is ranked. This information is provided to experts who can model the risk based on industry standard tools to illustrate the impact.

Third party tools can be used to develop risk reporting. Feeding data into these tools on the technology assets and the solution fingerprint can give a representation of the percentage of outdated end of life solutions in areas that are critical to operations. That report with metrics can be presented to the leadership of the risk areas. Years ago, outdated technology wasn't considered a huge problem if the equipment was still working. But today, if it's a security risk, then the conversation changes. There are third party vendors that can support outdated technology. But if it's not protected from a security perspective, then it's a risk.

To some extent, cyber insurers ask about tech debt and what's the acceptable tech debt ratio. If there are any major systems, we have to describe what other controls are in place to protect them. We haven't seen any major variances in policy. But insurers may turn around and tell organizations with huge security or technology debt that they won't insure them, or will charge high premiums, so that could become a challenging piece.

Human Capital

Another thing that should be taken into account when calculating cybersecurity debt is human capital. People get so used to doing the same old things and operating in the same old way. Identifying individuals who are capable of learning new things and ensuring that they get that training is a challenge that should be part of the same level of expectation that investing in technology is.

NAGOMI CONTRIBUTON

EMANUEL SALMONA

Co-founder & CEO, Nagomi

Nagomi's Investment in You: Because Cybersecurity Debt Shouldn't Be on Your Balance Sheet

Despite years of increased investment in cybersecurity, it's clear that more money doesn't always mean better results. Rather than staying ahead of threats, we're left with disconnected tools and processes. Our resources are spread too thin, and we keep reacting instead of making real progress. This is why Nagomi is proud to sponsor this report—to work with security experts on how to balance cybersecurity debt and finally get the results we all expect from our investments.

At Nagomi, we know that when teams are overwhelmed with too many tools that don't work together, they can't manage risk effectively. Other industries have found ways to improve efficiency, but the security industry has struggled because teams haven't had time to integrate tools in a fast-changing environment with growing vulnerabilities and an increasing number of tools. Not to mention, the talent shortage only makes things harder.

So, what's the solution? In my view, we're at a crossroads. Reducing cybersecurity debt isn't about cutting costs or adding complexity—it's about giving security teams the right tools and clarity to focus on real threats. When tools work together, teams can be confident that their defenses are working as expected. This gives them the ability to identify and communicate risk clearly to other stakeholders.

To make tools work together effectively, three things are essential. First, you need good visibility into the assets you're defending. Without it, it's hard to know if an asset is properly protected. Second, you need to ensure the tools you have are still providing the right capabilities. Cybersecurity evolves quickly, and some tools may no longer be up to the task. Third, and most importantly, you need to know if all the tools are running effectively against the risks you're facing.

At Nagomi Security, we're committed to helping organizations reduce cybersecurity debt by offering tools that simplify processes and connect everything together. This way, companies can reduce security backlogs, improve team collaboration, and move toward proactive defense. We may never completely eliminate cybersecurity debt, but we can make it manageable—and that's the key to getting real results from our cybersecurity investments.

Bio

Emanuel Salmona is the Co-Founder and Chief Executive Officer of Nagomi Security, bringing extensive international experience in cybersecurity and business leadership. Before founding Nagomi, Emanuel served as the General Manager of EMEA and Vice President of Global Partnerships at Claroty, a global leader in IoT and OT cybersecurity, where he helped drive the company's growth and strategic alliances.

Prior to his work at Claroty, Emanuel held several key commercial executive roles at Siemens across Germany, South Korea, and Switzerland, leading business operations and driving market expansion. His early career also includes service as an Intelligence Officer in the IDF Cyber Intelligence Unit 8200, where he developed a deep understanding of the intersection between security, technology, and business.

Emanuel holds an MBA from INSEAD, and his vision for Nagomi Security is rooted in his commitment to reshaping the cybersecurity landscape by delivering innovative solutions that drive business resilience and empower organizations to navigate emerging threats.

WORKS CITED

(in order of appearance)

Ozkaya, Ipek, et al. *Report to the Congressional Defense Committees on National Defense Authorization Act (NDAA) for Fiscal Year 2022 Section 835 Independent Study on Technical Debt in Software-Intensive Systems.* 2023, insights.sei.cmu.edu/documents/5806/Congressional_Report_Sect835_Tech_Debt_CMU-SEI-2023-TR-003.pdf, https://doi.org/10.1184/R1/24043392. Accessed 23 Feb. 2025.

Fairley, Richard E., and Mary Jane Willshire. "Better Now than Later: Managing Technical Debt in Systems Development." Computer, vol. 50, no. 5, May 2017, pp. 80–87, https://doi.org/10.1109/mc.2017.124. Accessed 23 Feb. 2025.

Siavvas, Miltiadis, et al. "Technical Debt as an Indicator of Software Security Risk: A Machine Learning Approach for Software Development Enterprises." Enterprise Information Systems, 24 Sept. 2020, pp. 1–43, https://doi.org/10.1080/17517575.2020.1824017**.**

Martini, Antonio, and Jan Bosch. The Danger of Architectural Technical Debt: Contagious Debt and Vicious Circles. 1 May 2015, https://doi.org/10.1109/wicsa.2015.31. Accessed 23 Feb. 2025.

"Cybersecurity Debt: A Ticking Time Bomb! - CyberExperts.com." CyberExperts.com, 27 Nov. 2021, cyberexperts.com/cybersecurity-debt/. Accessed 23 Feb. 2025.

World Economic Forum. "Bridging the Cyber Skills Gap - Why Is There a Cybersecurity Talent Shortage? World Economic Forum Centre for Cybersecurity." Weforum.org, 2024, initiatives.weforum.org/bridging-the-cyber-skills-gap/home.

The Cyber Hero vCISO Network GPT powered by Cyber Shield By Max Justice, PhD
A valuable cybersecurity tool for SMBs to shield themselves against the bad actors. https://chatgpt.com/g/g-pW5snOfvM-the-chn-vciso-gpt-powered-by-cyber-shield

Editor's Note: This section was created using the tool at https://www.mybib.com/tools/works-cited-generator

EXECUTIVE EDITOR

BOB TURNER

Penn State University

Bob Turner is the CISO at Penn State University with decades of leadership experience in telecommunications operations and technology, information security, cybersecurity consulting, business continuity planning and education. Bob supports CISOs as Lead Writer and Editor for Security Current's CISOs Investigate series. He is a board member and thought leader with numerous published articles on education, technology, information technology management, cybersecurity strategy and leadership. Bob is a retired Navy Communications Limited Duty Officer and served in submarines as Chief Radioman.

CONTRIBUTORS

JOHANN BALAGUER

Johann Belaguer is a cybersecurity expert with extensive experience in application and software security, cloud security, and security architecture. His expertise spans security operations, vulnerability management, penetration testing, and incident response.

Johann has a strong background in threat intelligence, third-party risk, cyber-crime investigations, and compliance. He also excels in project management, physical security, and M&A due diligence. Known for leading large teams and managing subject matter experts, Johann is skilled in security governance and auditing across complex environments.

DAVID CASS

David Cass is President of CISOs Connect, leading peer engagement for cybersecurity leaders. He is also Global CISO at GSR, a crypto market maker, where he oversees information security and privacy strategies. Previously, Cass was a Senior Partner at Law and Forensics and a lead regulator at the Federal Reserve Bank of New York. He has held roles at IBM, Elsevier, and contributed to major blockchain initiatives. David holds an MSE from the University of Pennsylvania and an MBA from MIT. He also teaches at Harvard and Rutgers.

CONTRIBUTORS

Alicia Clarke is the Head of Cyber Security, Risk, and Privacy at PGA TOUR Superstores. With 24+ years in cybersecurity across multiple industries, she leads the company's efforts to strengthen its security posture. Alicia has held key roles, including Director of Risk and Vulnerability Management at ACI Worldwide. She's been nominated for the 2024 Georgia CISO ORBIE® Awards and received the Accelerated Top 100 CISOs (A100) award.

Alicia is an active community leader and mentor, serving on various cybersecurity advisory boards and promoting diversity in her field.

ALICIA CLARKE

Nikk is a globally recognized CISO with extensive international experience, known for aligning cybersecurity with business strategy. At RWE, he secures operations while driving innovation. His career spans the US Army, NATO, Alstom, ConocoPhillips, and more. Since the early 2000s, he has championed security as a business enabler. A Ponemon Institute Distinguished Fellow and US Navy award recipient, he brings a business-first approach to cybersecurity, fostering resilient organizations where security fuels growth.

NIKK GILBERT

CONTRIBUTORS

Monique is a seasoned leader with over 25 years' experience in Cybersecurity, Risk Management, IT Governance, Vulnerability Management, and Incident Response. Her work has crossed multiple industries including Food & Beverages, Media & Entertainment, Transportation, Telecommunications, and Healthcare. She serves as Vice President of Information Security at Piedmont, Georgia's leading healthcare system. She is responsible for overseeing the security of electronic Healthcare information and content as it pertains to Piedmont's business, employees, and patient data.

MONIQUE HART

David Lackey is a seasoned Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO) with extensive experience in building and implementing comprehensive security programs, compliance strategies, and risk management frameworks. He excels in creating risk-based security programs that align with organizational goals and has guided organizations from startups to Fortune 500 companies. As a recognized visionary and thought leader, David is known for his strategic and proactive approach to solving cybersecurity challenges and building scalable and effective cybersecurity programs.

DAVID LACKEY

CONTRIBUTORS

Lock Langdon, VP and Chief Information Security Officer at Aprio Advisory Group, LLC, earned the prestigious CISOs Connect A100 award in 2024 for his exceptional leadership in cybersecurity. With senior roles at renowned organizations like Mayo Clinic, Stanford Children's Health, McKesson, and Splunk, Lock has a unique perspective on both client and sales challenges. He is dedicated to mentoring future cybersecurity professionals and actively collaborates with groups focused on enhancing national security. Looking ahead, Lock aims to continue advancing security programs and partnering with industry leaders to address evolving global security challenges.

LOCK LANGDON

Brian R. Miller is an experienced executive specializing in cybersecurity, IT strategy, and advanced analytics across defense, intelligence, and commercial sectors. Currently the CISO at Healthfirst, he leads enterprise security programs. Previously, he directed Booz Allen Hamilton's Cyber Security business, serving clients such as the Department of Defense, NSA, and NRO. Brian's expertise includes security architecture, risk management, compliance (NIST, FISMA), and incident response. He holds CISSP certification and has extensive experience in program management and consulting.

BRIAN MILLER

CONTRIBUTORS

Neda Pitt is a strategic security executive with over 22 years of experience modernizing IT systems and optimizing security management practices. She advocates for innovative information security and risk management to drive digital transformation and enhance business KPIs. A decisive, people-oriented leader, Neda excels in building high-performing teams to secure information assets, product technologies, manufacturing, enterprise IT, and third-party partnerships. Her expertise ensures comprehensive security across diverse organizational landscapes.

NEDA PITT

Hussein Syed is an experienced Chief Information Security Officer with a strong background in the healthcare industry. He is skilled in IT strategy, software documentation, and healthcare information technology (HIT). With expertise in information security, Hussein has a proven track record of enhancing IT systems to ensure the protection and integrity of sensitive healthcare data. His leadership and strategic approach help organizations maintain secure, efficient, and compliant technology environments within the healthcare sector.

HUSSEIN SYED

CISO FELLOW

Jake is a visionary business leader who brings 25+ years of global cybersecurity and digital trust leadership. He has a strong combination of proven experience, demonstrable results, and a compelling storytelling flare for customers, Boards of Directors, investors, and employees. He brings unwavering integrity, passion for relationships, decisive insight, and an ability to align resources and priorities. Jake works for Aristocrat Technologies, a $6B gaming and entertainment company where he serves as Senior Vice President and Chief Information Security Officer (CISO) focused on accelerating a powerful transformation of Digital Trust capabilities to deliver competitive differentiation, business value, and results.

JAKE MARTENS