Evolving Cybersecurity Essentials

A CIO Guide to Protecting the Enterprise

Foreword

Rapidly changing employee and customer expectations compel organizations to accelerate digitization efforts and build hybrid work environments. Unfortunately, these shifts add complexity and expose vulnerabilities that bad actors increasingly exploit with sophisticated attacks. This study aims to help CIOs by providing tactics, approaches, and advice from IT executives who successfully mitigate cyber threats. Our goal is to help organizations meet the evolving cybersecurity challenges that pose considerable risks.

The IT Media Group (ITMG) undertook this project with sponsorship from ActZero, a firm that actively partners with companies to drive security engineering, increase internal efficiencies, and build mature cybersecurity postures. ActZero specializes in monitoring, detecting, and responding to cybersecurity threats by leveraging data science, artificial intelligence, and machine learning.

This report contributes to ITMG's mission of supporting and adding value to the IT executive community. We provide a wide range of opportunities for direct engagement between IT vendors and industry executives, enabling them to share knowledge and opinions, provide thought leadership, build relationships, and engage in a dialogue of benefit to both parties.

For feedback or questions, contact:
Nasheen Liu, Managing Partner & SVP, CIO Program Strategy, The IT Media Group
nliu@theitmediagroup.com

Contents

Executive summary

Organizations expect their CIOs to protect enterprise data and technology assets from the growing volume of cyber threats. Unfortunately, the speed at which cyber-attacks emerge poses tough challenges for resource-constrained IT departments.

CIOs must bet on which solutions will be best at thwarting the threats to their organizations. However, this task is daunting without the skills and technologies to identify the right signals in a sea of noise. To be successful, IT leaders must develop a cybersecurity roadmap that allocates sufficient resources to protect the enterprise while improving operational efficiency.

Scope

This report guides CIOs through the evolving cyber threatscape and the most effective tactics and strategies for confronting it. We also outline the foundations CIOs should put in place to fulfill their security mandates. Finally, we provide an enterprise roadmap that utilizes the approaches described in this study.

Methodology

The IT Media Group leveraged its wide-ranging relationships with the CIO community to prepare this document. Our research included interviews with more than a dozen senior IT executives representing various industries across North America. We also examined ITMG's content repository and an array of external resources to substantiate our findings.

Key findings

Evolving cyber attacks pose severe threats to organizations across all sectors. Accordingly, successful IT leaders mitigate risks by implementing cybersecurity approaches that keep them ahead of their adversaries. These CIOs excel at narrowing the threat surface, or window of exposure, while ramping up the ability to detect and respond to attacks that penetrate their defenses.

We documented more than two dozen examples of how CIOs overcome cybersecurity challenges and achieve their business objectives. These leaders described the following essentials:

- Recognize that cybersecurity is a business problem requiring executive awareness and support.
- Adopt an outcome-based strategy that focuses on proactive preparedness and avoiding extortion.
- Deploy AI-enabled detection and response capabilities that operate at scale and at machine speeds.
- Embrace data-science principles to increase maturity and improve operations efficiency.
- Leverage the partner ecosystem to acquire talent, expand capabilities, and reduce time to results.

We encourage CIOs to explore the tactics and approaches described in this study. Our goal is to promote conversations between technology leaders and service providers and spur action that leads to positive business outcomes.

1 Recognize the evolving threatscape

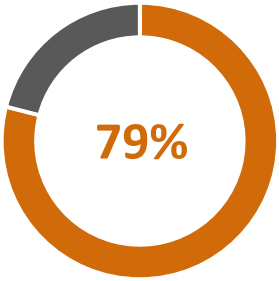
CIOs find themselves caught between digital transformation imperatives and a seemingly endless series of security crises. Moreover, their efforts to reduce complexity and improve governance have introduced potential weak links that draw increased scrutiny from inside and outside the organization. As a result, IT leaders must make robust cybersecurity an essential part of their overall strategies and answer the following questions:

- What evolving cybersecurity risks should be our focus?
- Are we doing the proper due diligence to protect ourselves from cyber-attacks?
- How do we verify the security of newly implemented technologies so that they won't be the source of a breach?

This report provides CIOs with a guide that answers these questions. It contains practical advice from 19 IT executives with a wealth of experience in implementing successful cybersecurity solutions. It also includes timely information from a wide range of research materials.

This section describes the evolving security challenges impacting modern digital organizations. Subsequent sections detail basic, advanced, and evolving approaches CIOs employ to address these challenges. Finally, the study concludes with a cybersecurity roadmap that brings all the concepts together.

1.1 Address the board's concern over cybersecurity



of companies incurred a financial loss due to lack of cyber-preparedness

"Boards remain concerned about reputation and operational stability, so we need to know what we're doing to stay out of the broadening cybersecurity spotlight."

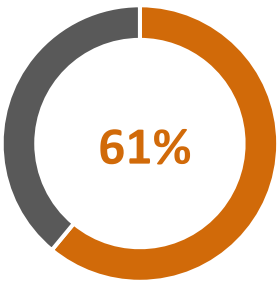
Helen Polatajko, Board Director

The accelerated pace of cyber-attacks poses an existential threat to organizations of all sizes in every industry. The increased volume and sophistication of attacks overwhelm beleaguered security teams and threaten transformation strategies needed to satisfy customer and employee expectations. The finding that 79% of companies incurred a financial loss or suffered some other setback due to their lack of cyber-preparedness underscores the urgency to act[1]. And boards expect action. They constantly ask their IT executives how they monitor the business, what they look at, and whether they have the proper protections in place.

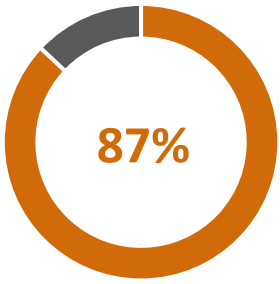
"Boards love to read what's happening in the world and compare themselves. But unfortunately, we see the rise of security incidents, and that concerns us," says Helen Polatajko, former CIO and an independent director on several boards. "Boards remain concerned about reputation and operational stability, so we need to know what we're doing to stay out of the broadening cybersecurity spotlight."

1.2 Tackle the escalating threat of ransomware

Ransomware attacks have grown in sophistication, expanding from endpoints and networks to the virtual cloud and containerized environments. At the same time, attackers have become more organized, deploying developer kits and platforms to broker ransom payments. They also use progressively harder to detect methods, rendering many older preventative technologies ineffective. Cybersecurity Ventures estimated USD 20B of ransomware damage occurred in 2021[2]. In addition, the breadth of these attacks is far-reaching, with 61% of businesses reporting that ransomware had hit them[1], equating to an attack every 11 seconds.



of businesses reported ransomware had hit them



of consumers won't do business with a company if they have concerns about its security practices

CIOs must deal with increasing ransomware impacts and maliciousness. For example, in Q2 2020, the average ransom payment was more than USD 178K per incident[3], with 34% of companies failing to get their data back after paying a ransom[1]. To add to the pain, attackers can exfiltrate private information resulting in further demands after the initial incident is considered closed.

In addition to the monetary outlay, organizations experience even more severe downstream business consequences. For example, the average downtime due to a ransomware attack is six days[1], and 87% of consumers won't do business with a company if they have concerns about its security practices[4].

For insights around these risks, we spoke with John Comacchio, Senior Vice president and CIO of Teknion, a build-to-order provider of high-end office furniture to the Fortune 2000. He explains, "Privacy is a major concern for our

customers. We include privacy rules in the RFPs and contracts we sign with them. We must contact them if we have an attack." Teknion focuses on prevention to avoid triggering these strict rules. Comacchio adds, "Even if you can contain an attack, you still wear the scarlet letter 'R' for ransomware." Emphasizing Comacchio's viewpoints, jurisdictions continue to enact demanding cyber breach notification laws. Our research found that ransomware is becoming the number one security concern because of increased attack volumes and the ensuing fallout. Impacted enterprises lose existing customers and lose faith from the entire community they serve.

1.3 Manage the extended enterprise

The growth of hybrid work and cloud computing has extended the enterprise beyond the office and the data center walls. This expanded infrastructure includes the proliferation of endpoints, consumer-grade networks, and cloud providers, all of which introduce a myriad of monitoring and security challenges.

Howard Holton, CISO and Enterprise Architect for Rheem Manufacturing, describes how the move to remote work impacted this century-old company: "We had zero work from home before. We went from having twelve networks that we needed to secure to about 6,500 networks we now need to be aware of. This has put a ton of pressure on our security resources." Holton explains that the company needs to determine if the user or contractor is the actual person they say they are and validate that individual's home network security, a far more difficult task than securing Rheem's own controlled facilities.

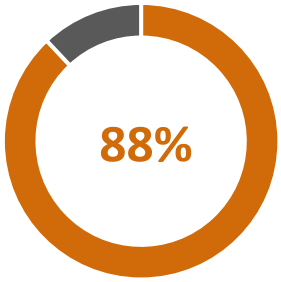
The extended enterprise is a consequence of implementing modern digital technologies and services. The following list summarizes examples of cybersecurity challenges CIOs must solve as they accelerate the digitization of the workplace:

Vulnerability point	Impact on the organization
Corporate firewalls	May be rendered ineffective in protecting remote employees unless they use a VPN.
Web gateways	No longer insulate the organization because remote workers use their own ISPs.
SIEM (Security Information and Event Management) services	May not have the ability to access remote logs and endpoints to determine if something malicious has occurred.
Public cloud services	Increasing zero-day exploits underscore the risk of public clouds. Gartner predicts that through 2025, over 99% of cloud breaches will have a customer misconfiguration mistake as the root cause[5].
Home networks	Could lack updated firmware, strong admin passwords, and robust security configurations, leaving them susceptible to attack.
Endpoints	The proliferation of mobile and computer devices outside the corporate network increases the attack surface and adds operational challenges related to security configurations, antivirus signatures, and identity management.

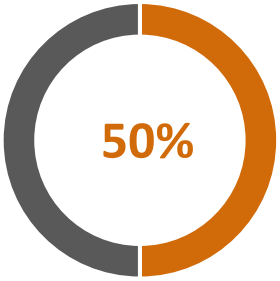
These impacts emphasize the importance of connecting all information regardless of asset location and type. Daniel West, Head of Mid-Market for cybersecurity firm ActZero, explains: "Legacy tools and data center designs have gone as far as they're going to go. To secure the expanded environment, organizations need to look at the products they

have, understand the known gaps, and find ways to close them." According to West, the extended assets a company has deployed now need to do the data center's work. That means implementing solutions that unlock the security potential of all the components of the distributed enterprise.

1.4 Learn how attackers exploit human psychology



of data breach incidents are caused by employee mistakes



of employees admit they made an error at work that could have led to security issues

Employee mistakes cause 88% of data breach incidents, and nearly 50% of employees admit that they were "very" or "pretty" certain they made an error at work that could have led to security issues for their company[6]. As a result, it is easy to understand why attacker efforts focus on the employee. Unfortunately, organizations can't expect the situation to improve soon because the move towards hybrid work will continue to create openings for social engineering attacks and deceptions.

"The increased sophistication of phishing attacks highlights the need for educational practices to train us for good hygiene and to teach us to become a tough target," says Monique Allen, EVP, Data & Technology at pension fund manager OMERS. She explains the challenges arising from the use of external warning banners on emails: "We become immune to them when we see them so frequently. Teams that do a lot of work with the external environment will get used to seeing the banner embedded in messages."

A lot of it is down to behavioral psychology, according to Andrew Wood, EVP Technology, at CAPREIT. The firm oversees 70,000 rental units and employs a diverse workforce to manage its portfolio of properties. Wood explains how the allure of an offer can potentially blind the recipient: "It's common to believe that [a security breach] will not happen to me. For example, if I click on a link, I get a reward, and it's not going to create a problem."

Research supports the assertions of Allen and Wood. A North American survey found that 25% of employees clicked on a phishing email at work[6]. These workers described the top reasons for clicking on potentially dangerous links:

- 43% perceived it to be a legitimate email.
- 41% thought that the email came from a senior executive within the company.
- 40% believed the email came from a well-known brand.

The surge in exposed credentials and compromised accounts indicates that employees remain incautious about their responsibilities at work and at home. As a result, CIOs must understand that cybersecurity is not a priority in the workforce, so they need to find new ways to reduce the risks and exposures caused by employee error.

1.5 Address security operations inefficiency

It is vital to make security operations effective and efficient at detecting and responding to threats. Unfortunately, high volumes and increasingly variable log data generated across the extended enterprise makes security efficiency a challenge. Another task is for security teams to incorporate threat data from actual attacks into models requiring constant tuning. It is not surprising that most organizations can't reduce the number of false positives while finding real threats in a sea of data.

Security analysts find it hard to distinguish threat signals from noise because most legacy technologies produce alerts that don't convey enough information about security risks, impacts, or priorities. Organizations have attempted to solve this through automated alerting, but this approach can increase false positives resulting in alert fatigue. Ultimately, these factors create an environment where it is easier to miss actual attacks.

> "The present and likely threats, and predicting what is coming next, is something most CIOs and infosec officers have a hard time identifying. They still don't have the tools to synthesize all of the data that can help them find what the right approach should be."
>
> *Adam Mansour, Chief Security Officer, ActZero*

The need to address security efficiency is a priority when cybersecurity talent is scarce and under heightened pressure to reduce IT budgets. We asked Adam Mansour, Chief Security Officer at ActZero, why this problem is difficult to solve. "The present and likely threats, and predicting what is coming next, is something most CIOs and infosec officers have a hard time identifying," he says. "They join forums, attend webinars, and engage their teams, but they still don't have the tools to synthesize all of the data with enough forward-looking intelligence that can help them find what the right approach should be." He adds, this can keep organizations one step behind the attacker.

ActZero's Daniel West provides additional insights gleaned from his experience working with dozens of organizations: "To be effective, you need to minimize the false negatives. For example, in a scenario where there is a long-cycle attack, organizations experience a broad set of weak signals spread out over days or weeks. Throughout the attack, there will be too many disjointed events for any human to find." This situation requires organizations to look at multiple data sources across their endpoints, networks, and clouds and then employ data science to achieve a high signal-to-noise ratio. According to West, this approach is challenging because most organizations don't have the required skills and technologies.

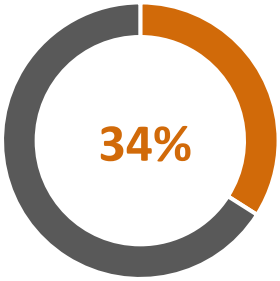
1.6 Mitigate the cyber insurance dilemma

Every public organization we researched includes a provision for cyber insurance in their annual report. Many of the IT executives we interviewed lamented rising premiums and the increasingly complex and arduous effort required to apply for and comply with their policies. Because of their industry and size, some companies that have never experienced a breach find themselves in the same high-risk category as less diligent firms when it comes time to renew.

>$178,000

Average ransomware payment[3]

Boards see cyber insurance as a means of mitigating the risk of ransomware. However, as we've described previously, the ransom is only a small part of the cost to the organization. Furthermore, the company's sense of security may be false, for attackers won't hesitate to use the firm's liability limit as a negotiating point.



of companies failed to get their data back after paying a ransom

Soon, there is the possibility that cyber insurance will be unavailable to all but a few enterprises[7]. This prospect exists because loss-ratios for insurers continue to climb even while premiums increase.

"The concept of cyber insurance applies the idea that the CIO doesn't know what bets to take," says ActZero's Adam Mansour. "The disruption occurring in the insurance industry demonstrates that even those in the actuary business won't take those bets either." Mansour explains that as insurers increase their rates or exit the business, they imply to their customers that they can't bet on them versus the adversary.

For these reasons, CIOs shouldn't assume that cyber insurance will largely mitigate their security risks. Instead, they must take additional actions to protect their organizations. The following section describes tactics and approaches that address the evolving threat landscape.

2 Include these approaches in your security strategy

CIOs must set up robust defenses that reduce the threat surface and enhance the ability to detect the attacks that get through. Cybersecurity effectiveness is dependent on the types of approaches organizations take as part of their security strategy. This section describes the basic, advanced, and evolving methods that leading organizations employ to stay ahead of the adversary.

2.1 Build strong defenses

A cybersecurity defense plan aims to achieve operational stability and business continuity. Chris Finan, COO of ActZero and former director for cybersecurity policy at The White House, describes the elements of an effective plan: "Risks to core operations require the plan to be holistic with key stakeholder buy-in. Organizations need to think in terms of risk management and risk transfer. This process starts with finding people who can harden systems. If you have the right restriction policies in place, along with proper hygiene and encryption, you're going to reduce the attack surface and make the problem a lot more manageable."

Howard Holton, CISO from Rheem, supports this approach: "I want to reduce the attack surface to the smallest possible footprint without impacting users so much that they can't get their jobs done." When asked how to accomplish this effectively, Holton explains, "I think of cybersecurity like Swiss cheese. A single slice has so many holes in it that it might as well be invisible, but as we add all the layers of protection, pretty soon you can't see through the block of cheese anymore."

"I think of cybersecurity like Swiss cheese. A single slice has so many holes in it that it might as well be invisible, but as we add all the layers of protection, pretty soon you can't see through the block of cheese anymore."

Howard Holton, CISO and Enterprise Architect, Rheem Manufacturing

Best practices prescribe a layered cyber defense plan to make it difficult for bad actors to infiltrate the organization. The elements of this plan include security hygiene, tactics to limit the human factor, and incident response planning. We spoke with over a dozen companies about the core approaches they use to address their evolving security challenges[8]. The following sections describe these approaches.

2.1.1 Practice security hygiene

During the rapid move to hybrid work environments, businesses prioritized functionality and operational speed over security considerations, causing a backlog of technical debt in the form of security hygiene issues. These issues may remain invisible until a breach or an exploit occurs.

The table stakes of a cyber defense plan include primary threat prevention. This area consists of the approaches that help shield the newly expanded enterprise from security breaches.

"We look at defense from the perspective of our SaaS providers, who can wreak havoc if they have an attack."
Eric Whaley, CIO, Wolseley Canada

"We look at defense from the perspective of our SaaS providers, who can wreak havoc if they have an attack," says Eric Whaley, CIO of distributor Wolseley Canada, a company with 210 branches and 2,700 employees. "All SaaS partners undergo a detailed security review to make sure they have the IT controls and processes in place should they get hacked." Whaley's approach provides an important consideration for organizations undergoing digital transformation. He adds, "We concentrate our roadmap around the cloud, SaaS, and how we protect ourselves from our vendors."

Andrew Wood of CAPREIT weighs in on another fundamental: "We've looked strongly at our backup strategy. It's not just a question of being able to protect the data; it's about being able to remediate the problem and recover in a timely manner." Wood's approach takes advantage of significant advancements in data protection solutions to address cyber threats. He explains, "We take offsite backups daily, so in the event of an attack that impacts us, we can rapidly respond and recover."

Vendor evaluation and data protection form part of a defense strategy. Below, we summarize the basic techniques used by leading organizations:

Security hygiene approaches
Evaluate the security profile of remote employee and contractor configurations.
Use air gap isolation and network segmentation techniques to limit malicious lateral movement across IT and operational technology (OT).
Implement a cloud access security broker (CASB) to improve security control over the growing number of private and public cloud services you use.
Heighten risk assessments and specify compliance criteria when onboarding vendors to secure the IT supply chain[9].
Design software restriction policies to prevent ransomware from executing in the environment. This approach provides some protection for known and zero-day exploits.
Create a program to deploy zero trust security throughout the organization.
Perform pro-active pentesting and external reviews of the infrastructure covering both OT and IT.
Put in place a robust backup strategy that focuses on data protection and fast recall/restore.

2.1.2 Limit the human factor

As stated, human error is responsible for the vast majority of data breaches. Unfortunately, despite focused efforts to address this exposure, employees remain susceptible to account takeover attacks (ATOs), which are increasing in frequency by 282% annually[10]. Often, ATOs represent the first step in a series of attacks within an organization to obtain privileged access, conduct fraud, and install ransomware.

282%

annual increase in account takeover attacks

Natalia Bakhtina, Director, Cybersecurity and IT Risk Management, at insurance provider BFL CANADA, explains the importance of educating the end-user: “Training is important. If there is an understanding that a single click can be the doorway to a breach, then users will be more attentive to the ramifications.” Furthermore, Bakhtina cautions against advancing the view that technology provides comprehensive protection. “By instilling the notion that tools can’t protect everything, users become more responsible for their actions, rather than being on the recipient side of a cybersecurity incident,” she says.

To address the human challenge, organizations should employ a combination of people and technology-centric approaches. Here is a summary of these methods:

Limiting the human factor
Implement ongoing user security awareness training and conduct phishing campaigns. Make the reporting of suspected phishing attacks easy and responsive.
Treat remote computing assets as disposable and limit data persistence. Consider using VDI technology.
Launch a “cyber heroes” program that rewards employees for helping improve cybersecurity.
Add encryption of mobile technology along with “find my device” and remote wiping. Install antivirus and antimalware tools and keep them up to date.
Standardize on a password manager to enforce strong passwords and to limit re-use.
Deploy multi-factor authentication (MFA) to reduce the impact of credential theft. Where possible, avoid SMS as a second factor because telecommunications companies remain susceptible to SIM card switching via social engineering.
Use VPN technologies to make it more difficult to intercept and collect data from network traffic for users outside the corporate firewalls.
Implement identity and access management solutions that apply rules and restrictions universally to all user accounts. Extend this approach to allow geo-conditional access to control logins by location.
Enable available email security features, including DMARC, safe link, inbound/outbound inspection, and mailbox scanning.

2.1.3 Plan incident responses

Defenses alone can’t reduce cyber incident risks to zero. Best practices dictate that organizations build a response plan to ensure the readiness of the troops when needed. We spoke with Marvin Wong, VP of Business Intelligence, Technology & Security at SECURE Energy, for advice on this topic. He explains, “We adopted the Incident Command System (ICS) approach for how we respond to emergencies in the field. We’re applying that methodology to technology because we want to respond to a cybersecurity incident consistently across our business.” Wong brings a wealth of experience from his tenure on the operations side of this energy services company. He adds, “We develop our IT playbooks to provide clarity on our tactical steps to lock down our systems quickly to limit the damage. The ICS process works in tandem to lead us through the entire life cycle of the event to ensure all teams are well-coordinated and focused.” The approach used by SECURE elevates cybersecurity to the enterprise level by requiring that IT and the business work together to solve their problems.

The following list summarizes the incident planning elements used by organizations:

Incident response planning
Regularly test and externally review plans to document response times and identify improvement opportunities.
Use scenario planning exercises to anticipate the disruption that attacks could cause.
Start with assets that threat actors will find the most attractive. Then, map out the attack surface and how adversaries could reach these targets.
Ensure planning has an enterprise scope, including vendors and partners.

2.2 Add advanced capabilities to the toolkit

As quickly as organizations implement their cyber defenses, attackers innovate to evade them. As a result, bad actors breach even the best protection. In addition, sophisticated adversaries no longer release their payloads right away; instead, they may lurk undetected inside the company network for days, weeks, or even months. During this time, they conduct surveillance and compromise critical assets to inflict maximum damage. The time between compromise and attack provides a window of opportunity to identify malicious activity and eradicate it. A smaller window is also available once an attack has started and begins to spread through the organization. Both intervals require organizations to shift their focus from reactive to proactive by adding advanced methods to their cybersecurity portfolio.

2.2.1 Implement detection and response

Standard signature-based tools may not detect zero-day threats, find attackers using already installed tools ("living off the land"), or identify adversaries using stolen credentials. Organizations need to incorporate detection and response across the expanded environment and continuously scan assets for vulnerabilities and malicious behaviour. Unfortunately, most enterprises don't have the human resources to sift through the massive amounts of unstructured logs and events to detect a wide variety of threats. In addition, once IT finds an attack, the organization may not possess the means to lock down the environment, analyze the threat in a lab, and develop measures to kill and eradicate it.

"Attacks move so quickly that there is very little time for humans to respond to them. So you need technology to detect breaches, stop them in their tracks, and then tell the humans afterwards," explains Sameer Bhalotra, CEO of ActZero and board member of more than a dozen cybersecurity companies. He adds that artificial intelligence (AI) and machine learning (ML) allow organizations to identify ransomware incidents, trigger automated responses, and inform end-users that an attack has been stopped or quarantined. "Forward leading AI provides the ability to detect a threat and trigger a response in real-time. Organizations need this because attacks move fast, impact every sector, and can be completely debilitating and lethal to a business," says Bhalotra.

"Forward leading AI provides the ability to detect a threat and trigger a response in real-time. Organizations need this because attacks move fast, impact every sector, and can be completely debilitating and lethal to a business."

Sameer Bhalotra, CEO, ActZero

CIOs should take heed of his guidance because the high volumes of data that organizations deal with are a top concern for their boards. Helen Polatajko provides insights from the boards she sits on: "We want the data because that's what we need to understand our customers and how to meet their expectations, but we also understand that data is a vulnerability. There is a limit to how effectively humans deal with all the noise that is coming in." Polatajko points to security personnel as the front line of defense but notes that there isn't enough cybersecurity talent available. "We believe AI is an enhancement to our staff," she says. "AI can be more agile and more adaptable. Boards become attached to this technology, and we ask our organizations how we complement our people on the ground with AI."

Successful CIOs ramp up AI-enabled detection and response capabilities to help secure the expanded environment's endpoints, network, and cloud components. This technique acts as insurance to quickly counteract a breach. In addition, IT leaders must exercise care to ensure that the selected approach adapts to the evolving threat landscape. This due diligence helps avoid the replacement costs for instrumentation and tuning if the solution doesn't meet the organization's security thresholds. With more than 100 vendors occupying this space, we provide guidance around what to look for in section 3 of this study.

2.2.2 Focus on active threat hunting

An essential part of a sound cybersecurity strategy is active threat hunting. This advanced approach requires intelligence analysts to investigate potential threats and compromises. ActZero's Bhalotra describes why active threat hunting extends cybersecurity capability: "Our SOC staff focus on threat hunting because we know that our AI can take care of a lot of the detecting and responding work they used to do. We need humans to dig around for attacks that we've not seen before, or AI is not detecting yet." He explains that this approach is possible because AI reduces the triage time of security operators.

"Most organizations configure endpoint detection and response tools for about 15 percent of what they should block so they won't break anything. The missing piece is proactive threat hunting, red teaming, and continuous testing of systems. Adding these capabilities will activate the remaining 85 percent of an organization's security products."

Daniel West, Head of Mid-Market, ActZero

Daniel West gives more reasons why this advanced approach is necessary: "Most organizations configure endpoint detection and response (EDR) tools for about 15 percent of what they should block so they won't break anything. The missing piece is proactive threat hunting, red teaming, and continuous testing of systems. Adding these capabilities will activate the remaining 85 percent of an organization's security products." West adds that the attack surface includes every place where credentials live. He cautions, "Without implementing dark web monitoring to identify compromised employee credentials, attackers will use reconnaissance to log in to different environments."

The art of threat hunting requires the allocation of analysts with the skills and experience to neutralize threats that target endpoints, networks, and cloud-based services. This approach complements detection by proactively investigating potential compromises, detecting advanced threats, and strengthening overall cyber defenses.

2.3 Examine evolving cybersecurity tactics

As threats continue to evolve, CIOs acknowledge that cybersecurity is an ongoing process requiring continuous improvement. After implementing the advanced approaches described in the previous section, organizations need to ensure that their own tactics evolve to stay ahead of the adversary.

2.3.1 Leverage data science to improve efficiency

Most companies face the following problems after they implement detection and response:

1. The growing volume of data, increasingly complex IT configurations and the need to counter a myriad of potential attacks overwhelm security resources. In addition, false positives lead to wasted effort and alert fatigue.
2. Instrumentation and AI models fail to raise critical alerts, increasing the organization's risk.
3. Lack of overall visibility across the enterprise fails to provide a complete picture of cybersecurity effectiveness.

> "To manage, you have to measure. You need scorecards that create actions for what you need to repair."
> *John Comacchio, CIO, Teknion*

A remedy for these issues is to tune configurations. Still, organizations find it challenging to achieve high-precision (more true positives than false positives) and high recall (the ability of the AI algorithm to return relevant results). The solution is to apply data science approaches. Says Teknion's John Comacchio, "To manage, you have to measure. You need scorecards that create actions for what you need to repair." Teknion leverages a cybersecurity rating system that highlights areas to address. This tactic helps to measure the effectiveness of their security efforts. He adds, "Buying tools and services that have this capability will allow CIOs to look at a scorecard and start to assess what they have to do and dig deeper into."

Adam Mansour provides insights around using data to improve prevention based on his experience with companies across North America: "A lot of enterprises attempt to increase efficiency in the absence of data. CIOs find it difficult to predict what's going to happen next, what's the most popular attack right now, and what they need to be stopping." Mansour explains that the answers to these questions require a data-driven approach that combines vast amounts of external threat data with a company's internally generated data. He adds, "We shouldn't make the next bet randomly because there's a lot at stake for CIOs. Instead, we focus on the ways organizations get hacked by identifying the right places to apply particular solutions within the data sets we collect on their behalf."

A data-driven approach requires that traditionally separate groups - cybersecurity engineers and data scientists - work together to detect anomalies[11]. If done effectively, the merger of the two disciplines allows threat hunters to determine missing data in existing models. In addition, it helps data scientists find ways to automate responses based on their insights into threat investigations. Our research identified several evolving metrics that help determine the efficiency of detection and response. As a result, organizations should consider the following measurements as part of their data-driven strategy:

Metric	What it measures
Remediation effectiveness	Proactive hardening actions to reduce the threat surface available to hackers.
Coverage and ingestion efficiency	The diversity of data sources and the volume of logs analyzed using ML to find attackers.
Detection model precision	False positives generated versus the number of actual attacks detected.
Signal-to-noise ratio	The number of features and variables used to detect an attack. Improving this metric helps to reduce false negatives - weak signals spread out over days or weeks that appear to be disjointed - that provide indicators of a breach when analyzed together.
Response effectiveness	The elapsed time between incident detection and the return to normal operations.

Machine learning algorithms and AI provide the underlying delivery mechanism for increased operational efficiency. The combined data science and cybersecurity team must test and refine these models as part of a data-based security framework. For optimal results, organizations should leverage multiple models. To help understand the scope of this work, here's a list of ML models included in this approach:

ML model type	What it's used for
Anomaly detection	Finding new attacks and attack families.
Supervised models	Capturing signals of existing attack types.
Holistic models	Detecting weaker signals spread out over different data sources and time.
Environmental models	Improving the signal-to-noise ratio by producing high-quality alerts. These models also suppress false positives to reduce alert fatigue.

Efficient cybersecurity operations identify suitable data sources to feed into machine learning algorithms to find threat signals in a sea of noise. Unfortunately for most organizations, the costs to attract and retain data scientists and cybersecurity personnel make these objectives difficult. The next section recounts how IT executives implement the cybersecurity approaches documented in this study.

3 Leaders describe cybersecurity essentials

Investing in every advantage to be gained through people, processes, and technology is critical to making headway against attackers. The faster the enterprise can block and detect an attack, the more it minimizes the harm.

"Our resiliency is dependent on a number of extended relationships with vendors to help us with our employees."
Maria Aiello, Global Head, Real Estate & Mortgages Technology, Manulife Investment Management

Successful organizations adopt a defense-in-depth approach, recognizing that there will be an attack at some point. To prepare themselves, companies must look at all the layers that need protecting. This is particularly true for financial services companies, which face a growing multitude of sophisticated adversaries. Maria Aiello, Global Head, Real Estate & Mortgages Technology at Manulife Investment Management, explains how they address this challenge: "Our resiliency is dependent on a number of extended relationships with vendors to help us with our employees. Accountability rests with all of our relationships. It's not one person who is accountable; it's the board, our employees, and our vendors who contribute to our resilience."

The following section describes how organizations implement their cybersecurity approaches. Senior leaders offer guidance and advice around creating a rigorous security strategy.

3.1 The role of the business-focused leader

Leadership plays a crucial role in implementing a comprehensive cybersecurity strategy. Martin Jepil, Global VP of Enterprise Architecture, at property management firm Avison Young emphasizes this: "Cybersecurity is led by one of our board members because it is important to our company. We believe that cyber risks are not an IT problem to solve. Our company is data-driven with many moving parts, so it makes sense to have a security roadmap in place." Jepil says that they use the roadmap as the action plan for the entire enterprise. "That is one of the reasons why the board drives it. All IT, management and other organizational action plans fall within our overall cybersecurity roadmap." Jepil explains that the company will be outsourcing the capabilities they don't have but will continue to manage the overall security strategy.

"Cybersecurity is led by one of our board members because it is important to our company. We believe that cyber risks are not an IT problem to solve."
Martin Jepil, Global VP of Enterprise Architecture, Avison Young

Chris Finan supports this leadership approach: "The C-suite and the board must understand the challenges and that first and foremost, cybersecurity is a business problem. Ultimately, it comes down to people finding ways to mitigate and transfer risk to execute well. The core of a great cyber defense is people." Finan recommends that leaders measure and prioritize to help their teams manage their capacity. He also encourages CIOs to let people enjoy a work-life balance because they will have more energy to be creative and problem-solve for the organization.

3.2 Building the defenses

The first phase of a cybersecurity strategy is implementing the defenses that reduce the threat surface and block attacks. At this stage, companies allocate a budget to implement safeguards that protect the organization from intruders. CIOs pursue an outcome-based strategy to prevent business compromise and avoid extortion via ransomware.

Budgetary constraints may impede the ability to acquire tools and the staff needed to operate them. Organizations can choose to buy a handful of tools or engage a service provider to secure a broader spectrum. Regardless of the selected option, companies must invest in holistic approaches that provide basic security hygiene, limit the human risk factor, and create initial incident response plans as described in Section 2.1.

3.3 Adding AI and ML-enabled detection and response

Most IT leaders believe a security breach is inevitable despite significant investments in defenses. As a result, organizations must allocate a sufficient budget for proactive detection and response to counter those breaches. The critical enablers for this approach are AI and ML. Over recent years, security providers have matured these technologies so that they can be applied at scale to help address the shortfall of cybersecurity talent.

> "Adding AI and machine learning gives our employees an edge and bolsters the human factor. We deploy AI and ML to look for abnormal activity."
> *Monique Allen, EVP, Data & Technology, OMERS*

"Adding AI and machine learning gives our employees an edge and bolsters the human factor," says OMERS Monique Allen. "We deploy AI and ML to look for abnormal activity." She explains that the technology finds patterns that seem valid at first but have unusual characteristics that trigger further investigation.

AI and ML use sophisticated algorithms to recognize activities that match dynamic indicators of a compromise. The technology works at speeds unattainable by traditional security systems and human-based operations.

3.4 Integrating data science with cybersecurity

The IT executives we spoke with say they still grapple with inefficiencies and ineffectiveness in stopping adversaries. Their challenges lie in the sophistication of attackers, the growing attack surface, and the need to manage high volumes of complex data.

CIOs progressively turn to data science to increase cybersecurity maturity, achieve higher signal-to-noise ratios, and continuously improve detection and response. This strategy calls for using the best people combined with modern AI algorithms. Organizations require a formal collaboration between the Chief Analytics Officer and Chief Security Officer. Their goal is to adopt an outcomes-based approach to develop the analytical models that improve cybersecurity performance and report on the metrics described in Section 2.3.1.

"CIOs who effectively incorporate data science with cybersecurity realize savings in time and money while building trust and confidence with the business," notes Sameer Bhalotra. He adds that efficiency also reduces senior leader overhead because they don't have to deal with the compliance and procedural headaches caused by false alarms. "At the end of the day, data enables agile detection and response to fast-moving attacks like ransomware," he says. "Additionally, lower false-positive rates result in productivity gains by reducing SOC operator burnout and turnover."

"CIOs who effectively incorporate data science with cybersecurity realize savings in time and money while building trust and confidence with the business."
Sameer Bhalotra, CEO, ActZero

3.5 Creating an outsourcing and partner strategy

People remain critical to executing cybersecurity strategies. Companies intent on building their cybersecurity capability must take the thorny path of hiring data scientists, AI specialists, security engineers, and operators who have experience running large teams of defenders. Once assembled, the organization must allocate the time to build and continuously upgrade the required tools, visualization capabilities, and security processes. Unfortunately, most organizations don't have the resources to compete for security talent in the current competitive market. With these challenges, it is no wonder that 100% of the companies we spoke with were already using or actively planning to outsource cybersecurity.

Companies need to think about this from a budgetary, recruiting, operations, and timing perspective. Says Rheem's CISO, Howard Holton, "I'm a big fan of outsourcing cybersecurity to companies that have a hundred times the SOC engineers that I should have and who actively look at the data and aggregate it down to their toolsets. I want to take

advantage of those ecosystems of capabilities and bring them into my organization." Holton provides a popular view of how organizations achieve proficiency that they can't replicate in-house. By outsourcing, enterprises also benefit from the continuous investments in hiring, credentialing, and upskilling required to stay ahead of evolving threats.

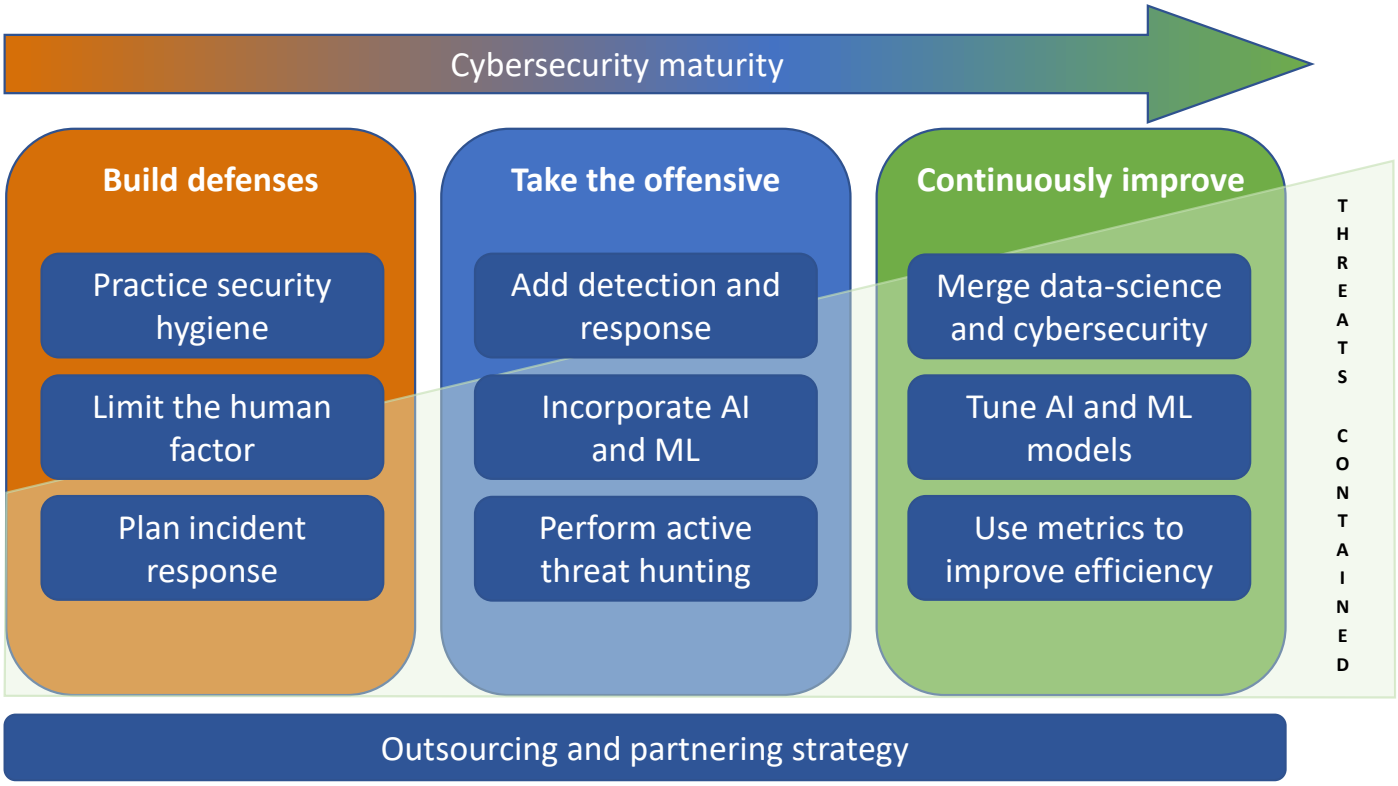
The cybersecurity space is evolving rapidly, with new providers entering the market with innovative offerings. At the same time, the boundaries separating the different kinds of managed security providers are increasingly becoming blurred. With more than 100 companies offering managed detection and response, the challenge for organizations is how to evaluate their options. Complicating the challenge is the relative newness of the metrics that measure efficiency and the reluctance of both vendors and customers to disclose their private data.

Here's a summary of the characteristics that drive AI-enabled detection and response efficacy. Organizations can use these criteria to assess the capabilities of their existing and potential security providers:

What to look for	Why it's important
Types of ML models	Impacts the number of incidents detected and their associated responses.
Age of the AI technology	Allows verification of the maturity of AI algorithms that require years of development before they work at scale.
Diversity and size of historical data	Improves detection accuracy for various threats across different industries.
Service coverage and log sources	Confirms detection across endpoints, networks, and the cloud services of your enterprise. Increases the ability to correlate weak threat signals across multiple assets.
Tuning and customization	Permits false positives in your environment to increase operational efficiency and adapt to changing conditions.
Detection efficiency metrics	Verifies signal-to-noise effectiveness and demonstrates the use of a data-based security strategy to improve operational efficiencies.
R&D expenditures	Confirms commitment to ongoing development to address evolving threats.
Staffing profile and experience	Validates ability to operate and improve the service to stay ahead of adversaries.
Partner ecosystem	Identifies extended capabilities and services that you can add to your cybersecurity toolkit.

4 Adopt this roadmap to protect the enterprise

Our research revealed that security challenges are similar regardless of industry. As a result, it is possible to provide a practical cybersecurity roadmap for any organization to follow. We have summarized the approaches detailed in this study in the roadmap below. The chart shows how the ability to defend, detect and respond to threats increases as the organization's security posture matures. Underlying the execution of the roadmap is an outsourcing and partnering strategy. CIOs who successfully implement an enterprise cybersecurity strategy will protect their organizations from harm while realizing positive business outcomes.



"When I think of how executives solve their cybersecurity challenges, I recognize that it's a team sport, where companies leverage specialization to realize their risk mitigation objectives," says ActZero's COO, Chris Finan. The path to achieving these goals is to implement AI-enabled cybersecurity protection and data science to deliver outcomes at machine speed across the digital enterprise.

Enjoy a secure digital transformation journey

ITMG was delighted to conduct this research project and speak with many IT leaders across North America who successfully defend their organizations against evolving cyber threats. As CIOs execute their digital transformation strategies, we invite them to examine the use cases and tactics covered in this study to keep their businesses safe.

References

1. Securing the Enterprise in the COVID World, 2020 survey of 1,175 global respondents in 10 countries, Mimecast
2. Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2021, 2019 article, Cybersecurity Ventures
3. The Coveware Quarterly Ransomware Report, Q2 2020 report, Coveware
4. The Consumer-Data Opportunity and the Privacy Imperative, survey of 1,000 North American consumers, McKinsey & Company
5. Is the Cloud Secure, 2021 predictions, Gartner
6. Psychology of Human Error, OnePoll survey of 2,000 working professionals, Tessian
7. 2022 Cybersecurity Predictions & 2021 Year in Review, 2022 White Paper, ActZero
8. The CIOs Evolving Cybersecurity Imperatives, 2021 roundtable, The IT Media Group
9. 6 Steps to Secure your IT Supply Chain, 2021 White Paper, ActZero
10. Account Takeover Fraud and the Growing Burden on Business, Q3 2020 digital trust and safety index comprising more than 34,000 sites/applications and a survey of 1,000 consumers, Sift
11. Understanding Machine Learning Models for Cybersecurity, 2021 Podcast, The Data Standard

The IT Media Group serves the IT management community by creating great resources for CIOs and producing events that enable IT executive peers to share knowledge, opinions, and best practices.

For more information, please visit:
theITmediagroup.com

Sponsored by ActZero