INFORMATION WEEK

July 2024

Tools and Technologies for Managing Cyber Risk in 2024

Brought to you by informa tech

INSIDE:

FEATURE

11 Ways to Manage Cyber Risk in 2024

Some oldies and goodies, and more than a few newbies, too – what matters is what's working!

By Pam Baker

As is to be expected, new security tools are piling atop of old ones and each is hawked as the best thing since sliced bread. Unfortunately, some of them will eat your lunch and do little to curb the bad guys' appetite for your company data. But some are truly helpful in the ongoing battle against the hungry hordes seeking to devour data and company riches. And just because a tool is new does not necessarily mean it's better – or worse – than those that came before.

"Overall, my favorite tools for managing risk are those that allow us to be proactive in our approach to managing risk and security. I would much rather find security problems before adversaries than after those adversaries are already wreaking havoc on our systems," says Brian Callahan, PhD, a Lecturer and Graduate Program Director at Rensselaer Polytechnic Institute's Information Technology and Web Science program.

The real test of these tools is how they perform on the frontline and in the hands of battle-tested cybersecurity pros. Here is what a few of them had to say about which tools and tech are making the cut in 2024.

1. MLOps Versus the GenAI Gorilla

GenAI is capable of helping hackers in many ways from perfecting phishing emails to designing prompt injections that spread malware automatically and change so swiftly that they're almost impossible to deflect. The field is still emerging in the mainstream and the defenses are too. That means there isn't a sufficient range of tools and tech to universally

protect against this new menace.

However, there are new tools that are proving beneficial against some variations of these types of threats.

"MLOps plays a crucial role in AI governance by bridging the gap between data science, engineering, and operations teams, ensuring that AI systems are developed, deployed, monitored, and maintained in a responsible and efficient manner," says Phani Dasari, Chief Information Security Officer at HGS, a global digital customer experience (CX) provider.

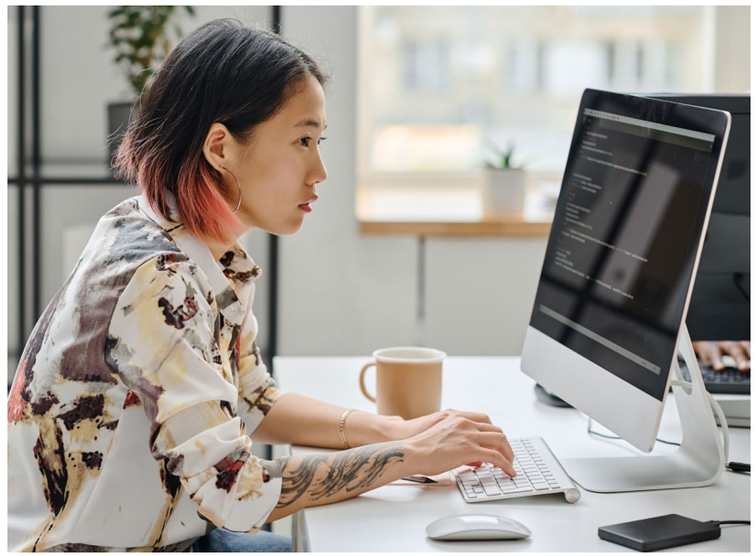
2. Tools for Locking Down the Network

Networks are constantly under attack. Finding efficient tools to protect them from an ever-changing onslaught of attacks is an ongoing challenge.

"Network mappers and packet capture tools top my list in the network protection category. It is impossible to defend networks when you don't truly understand what devices are on those networks and what kinds of traffic exists on your networks. These tools when combined provide us a clear understanding of what it is we need to manage and how we can best manage," says Callahan.

Challenges in protecting networks continue to shift in the direction of workforce trends too. Employees can be located anywhere today – and anywhere else tomorrow.

"A network tool that can provide better WiFi network access control, and built-in security options, like SSO, two-factor authentication, and more is key," says Richard



Jonker, NETGEAR's Vice President of Commercial Business Development, AV-over-IP, APAC & EMEA.

3. Managed Security Service Providers (MSSPs) Remain Popular

Given inflation and other economic uncertainties, companies both small and large are finding managed security service providers (MSSPs) to be a good bargain and a good return on investment.

"Financial institutions are prime targets for cybercriminals due to the nature of the data we collect, manage, and process. However, small and mid-sized credit unions typically don't have the same amount of resources as large national banks, even though we are responsible for protecting the same type of private information and financial data for our members," says Linnie Gooch, CTO at Foothill Federal Credit Union.

"Because of this, staying on top of the latest cybersecurity threats and evolving cybersecurity landscape has become a prime focus for the IT team. To do so effectively and efficiently, we decided to invest in a security operations platform and MDR services with a threat research team that is available 24/7 and enterprise-grade capabilities that work as an extension of our IT and security team," Gooch adds.

4. Top Software Fixers

In many ways, software is the soft underbelly of any organization and a prime target for data thieves.

"Static analysis tools, fuzzers, decompilers top my list for this category of protection. Even the best designed and implemented software will have bugs. Reading code and running the code in a development environment with an eye towards spotting those bugs can go a long way to get fixes out before adversaries can exploit them," says Callahan.

5. SIEM Is Still Holding Strong

"Any vendor who claims their tool or platform alone is the best tool is a vendor to stay away from," says Steve Tcherchian, CISO of XYPRO.com, a leading Simi-Valley based cybersecurity solutions company.

Tcherchian and others cite Security Information and Event

Management (SIEM) as key security tools to include in your defenses this year.

"SIEM tools, such as Splunk, IBM QRadar, LogRhythym and others aggregate and analyze log data from various sources to provide real-time monitoring and alerting," Tcherchian explains.

6. Haveibeenpwned Still Hasn't Been Pwned

Half the battle is knowing when you need to take up arms and forewarned is forearmed!

"I would say the best cyber security tool is Haveibeenpwned – it's a fantastic website and API that tells you if an email address, or even your password, has been compromised in a data breach and where that data breach occurred. If you discover that you've been affected, you can then take the necessary steps to overcome the breach and mitigate future risk," says Bryn Jones, Technical Director at digital agency Reckless, an ecommerce agency and software development firm.

7. Asset Intelligence Tools Are Looking to Be a Smart Choice

"As a CISO, I am responsible and held accountable for the internal security of every asset across our enterprise network – this includes devices, software, third-party applications, and collaboration tools. Additionally, I run our managed security practice that handles full-scope security for technology-based solutions, GRC consulting, offensive security, and more," says Brian Brown, CISO at Solis Security.

Brown says managing that many assets requires specialized tools that not only detect threats but tracks the fixes too. "Asset intelligence tools, like our partner, Sevco Security, provide my team with the visibility needed to fully understand the risk and business impact of unknown devices, users, software, and controls. Additionally, Sevco's unique exposure management capabilities uncover and track the remediation of unaddressed security vulnerabilities on both our network and our customers' networks to ensure that our security practices are proactive and effective," he adds.

8. DLP Rides Herd on Data Transfers

"Data loss prevention (DLP) tools help organizations prevent the unauthorized transmission of sensitive data outside the corporate network. They can monitor and control data transfers, enforce encryption policies, and prevent data leaks," says Vijay Alilughatta, COO of Zensar Technologies, a cybersecurity services company.

While DLP is a top tool in his arsenal, Alilughatta reports other tried-and-true tools are on his list too, such as encryption, access control, and data masking.

9. AI Model Wrangling Tools

Managing models is difficult given how fast they evolve and how quickly they pile up in any given organization. But

> **"My favorite tools for managing risk are those that allow us to be proactive in our approach to managing risk and security."**
>
> – Brian Callahan, PhD, Lecturer and Graduate Program Director
> Rensselaer Polytechnic Institute's Information Technology and Web Science program

guarding the integrity and security of each to preemptively address emerging threats such as Model Evasion, Model Inversion, and Membership Inference is an entirely another level of hard.

"Model management ensures the responsible development, deployment, and monitoring of AI models throughout their lifecycle, from development to deployment and retirement. They help track model versions, monitor performance, and ensure AI systems are deployed and maintained effectively," Dasari explains.

10. Safety in Numbers: ISACs, CVEs, OSINT

Sharing information among cybersecurity teams and professionals across many organizations is imperative to increasing the safety of each and all. Information Sharing and Analysis Centers (ISACs) are non-profit communities centered on this purpose. Common Vulnerabilities and Exposures (CVEs) databases, and open-source intelligence (OSINT) are also excellent sources to learn which tools and techs are working against current and emerging threats.

"This is where Information Sharing and Analysis Centers (ISACs) come into play. Most sectors have their own ISAC to best share industry-specific information quickly and effectively. The CVE system is a protocol for disseminating flaws in software. Anyone can search the database of CVEs and find known vulnerabilities against the software they are using, and steps to take to mitigate those vulnerabilities. It is the tool of collaboration that best helps ensure a safe and secure global landscape," says Callahan.

11. Identity Security Makes an Entrance and IAM Is Up for Review

After the massive Okta breach, IAM got more than a little side-eye from, well, nearly everyone whether they were an Okta customer or not. IAM simply went from golden to smoldering after one headlining fails too many. However, since chucking the concepts of authenticating users and limiting access makes no sense whatsoever, slathering on more protections seems the way to go.

Which is to say that 2024 is a great time to start revamping your IAM set-up. Just be sure to keep the mission in mind:

"IAM ensures only authorized users access sensitive data, reducing the risk of insider threats and compliance issues," says Tcherchian.

Remember that IAM is a program, not a project. It was meant to contain layers of protection all along but here we are. Enter a wave of new strategies around security, identity, and governance. The term for this new and improved approach is "identity security" and IAM has a role in that. So, yes, the revamping of IAM is still on your to-do list this year.

FEATURE

What Is AI TRiSM and Why Is it Time to Care?

Fearing renegade AI projects in user departments or applications tainted by flawed data, organizations are looking for a bit of structure in their AI initiatives.

By Mary E. Shacklett

Artificial intelligence trust, risk, and security management (AI TRiSM) is a technology and policy framework for managing AI. It's gaining traction in enterprises as they grapple with the questions of how, when and where to best use AI, while also keeping the AI compliant and reliable.

This is not an easy task.

The Challenges of AI Adoption

Short on AI skills, many organizations begin their AI journeys by relying on vendors and outside business partners to provide turnkey AI solutions. These systems manage IT operations, financial and healthcare databases, weather forecasts, website chat sessions, and other functions.

For many companies, this strategy of outsourcing AI isn't likely to change, because they don't have the in-house expertise or the financial resources to invest in AI on their own. For other companies where AI is both strategic and affordable, they need to trust the goodness of their own AI models, data and results.

In both cases, there is a responsibility for AI. That means asking key questions: Is the AI trustworthy? What are the risks of using AI if it fails? Is the AI secure?

The Central Role of AI Trust, Risk, and Security Management

The goal of AI TRiSM is to place the necessary trust, risk and security guardrails around AI systems so that enterprises can ensure that these systems are accurate, secure and compliant.

This can be a daunting undertaking, for while there are many years of governance experience and best practices for traditional applications and structured system of records data, there are few established best practices when it comes to managing and analyzing AI structured and unstructured data, and their applications, algorithms and machine learning.

How, for instance, do you vet all of the incoming volumes of data from research papers all over the world that your AI

might be analyzing in an effort to develop a new drug? Or how can you ensure that you are screening databases for the best job candidates if you are only using your company's past hiring history as your reference?

Let's Take a Closer Look at the AI TRiSM Framework

AI TRiSM addresses these questions with a framework for managing AI data and systems. This framework includes the following four elements:

- AI Explainability
- AI Model Operations
- AI Security
- AI Privacy

The goal of AI TRiSM is to place the necessary trust, risk and security guardrails around AI systems.

AI Explainability

If you use AI to obtain results and then draft a report to the board, do you feel secure when someone asks you how you arrived at your conclusion and what data sources were used?

It's a big question that encountered the school of hard knocks in 2018, when Amazon de-implemented an in-house AI recruiting system that disproportionately favored male over female job applicants.

Upon closer examination, the company realized that the only data it had fed to the AI system was from its own internal employment database. That data showed that in past years, the company had hired more males than females. Consequently, the company missed out on a large pool of qualified female applicants.

Next Steps for Implementing AI Explainability

No one wants to stand in front of their board trying to explain how AI went wrong. So, a best practice is to assure that you have a broad enough data source base for your AI before you run it. Equally important is that you cross-check your AI queries and algorithms to ensure that they are as inclusive and non-biased as possible.

The ultimate test is within yourself. If asked, can you confidently explain to yourself how the AI derived its conclusions, and what data it used to arrive at results?

AI Model Operations

After deployment, AI must be maintained. The challenge for enterprises is how to maintain it.

With systems of records, you perform maintenance by continuously monitoring performance and fine-tuning as needed, and by resolving software bugs when they occur. This form of maintenance has a running history of over 70 years, so there is no confusion about how to perform it.

In contrast, AI systems have few established maintenance practices. When AI is first deployed, it's checked against what subject matter experts in the field would conclude, and it must agree with what these experts conclude 95% of the time.

Over time, business, environmental, political and market conditions change. The AI application (and its conclusions) must change with them. This is where AI maintenance comes in.

Next Steps for Implementing AI Maintenance

If an AI system's outcomes suddenly decline in accuracy from 95% to 85%, it's time for a cross-disciplinary team of user subject matter experts and IT/data science to get together to see if data sources, algorithms, machine learning, etc., must be fine-tuned so they can re-align with the business and get back to the level of accuracy that the enterprise expects.

If AI maintenance isn't regularly performed, AI system results will lose accuracy. This increases company risk because the outcomes that management decisions are based upon could be wrong. Incorporating the AI TRiSM framework is designed check this.

AI Security

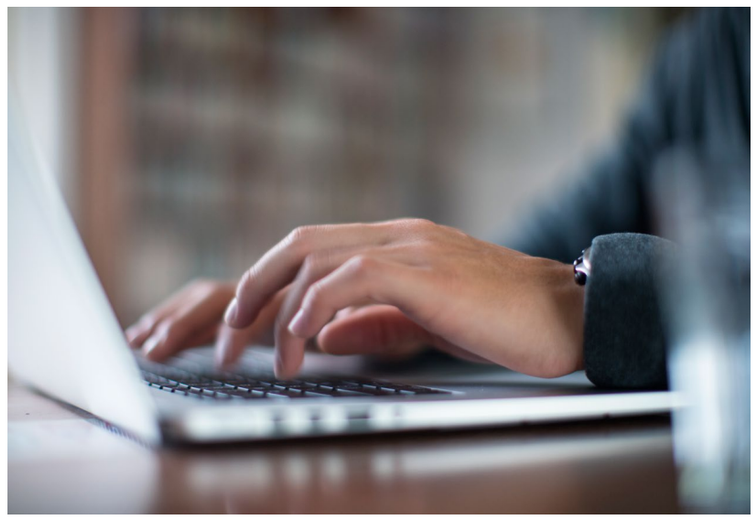
Hackers are finding new ways to attack AI systems as deployments grow.

One line of attack is data poisoning. This happens when a hacker gains access to AI model training data and corrupts the data, so the system produces erroneous results.

In AI security, AI TRiSM assumes that traditional IT methods of AI security enforcement are already in place. These include setting high authentication standards for AI users that include multi-factor authorization, building zero-trust networks and network segment boundaries around AI systems that further constrain access, and securing hardware, operating systems and applications. However, a second tier of AI security enforcement is also needed, which AI TRiSM addresses.

Next Steps for Implementing AI Maintenance

This second security front involves the vetting of all data source providers for AI projects. The goal is to ensure that each provider meets or exceeds enterprise governance and



security standards. IT should use additional data preparation tools to ensure that all data entering into an AI data repository has been cleaned, formatted and properly prepared for use.

AI Privacy

Enterprises have their own data privacy policies, but with AI, it's also necessary to ensure that the data brokers whom you purchase data from have similar data privacy policies. Focusing on this is core to the AI TRiSM framework.

For example, a large healthcare lab wanted to study the impact of cancer treatments on a variety of patients from Europe. It contracted with a number of hospitals and clinics to obtain patient data. The stipulation made to each data provider was that all patient health data was to be anonymized so that patient privacy was protected.

The lab obtained the variegated data from hospitals and clinics that it had asked for, and the data could be analyzed by geographical location, type of cancer, age and gender. However, there were no individual patient identifiers present in the data. All data providers had anonymized patient records to protect the privacy of patients.

The Future of AI TRiSM

Gartner says that by 2026, 80% of companies will be using technologies like generative AI, but few enterprises have inked the words "AI TRiSM" on their IT strategic roadmaps.

The good news is that many companies are already performing the steps that AI TRiSM enumerates. Enterprises are designing tightly orchestrated use cases where AI can benefit the business. They are actively deploying security measures like zero-trust networks and are doing a better job of vetting data brokers for security and data privacy compliance.

One lagging area is AI system maintenance and fine-tuning, but this is likely to garner more attention as more AI gets deployed.

Meanwhile, CIOs should start thinking ahead about what their IT audit and regulatory checklists are likely to look like in five years. You can expect auditors and regulators to come in with AI TRiSM checklists, and IT must be ready to check off all the boxes.

SPONSORED

The Core of Enterprise Security and Mitigating Risk Is Identity

A centralized approach to managing all types of identities and their access across diverse IT environments can simplify security, mitigate risks, and prevent costly breaches.

By Rex Booth, CISO, SailPoint

When we're not obsessing about identity security at SailPoint, we chat about all sorts of awesome topics – cars, gardens, travel, etc. But to stir things up, step into our astronomy channel, ask people for their favorite astronomer, and watch as the sky-enthusiast passions fly! It's always a close match, but our reigning champion is the 17th Century German astronomer and mathematician, Johannes Kepler.

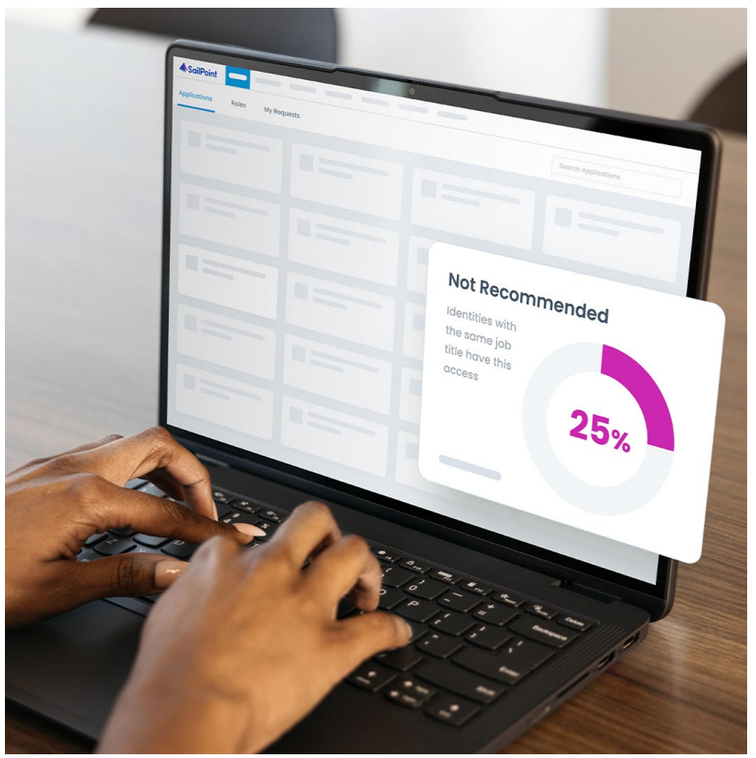
Kepler was a true genius, a polymath, a brilliant thinker who managed to express his big ideas with singular clarity. His discoveries literally changed the world. One of Kepler's most famous quotes is: "Nature loves simplicity and unity."

At SailPoint, we couldn't agree more. In an increasingly complex world, the best things are those that are simplified and unified. Which is why we strive to simplify and solve complex problems with unified identity solutions. Solutions that put identity at the center of your enterprise security orbit.

The Complexities of Modern Identity Security

Identity was always essential, but it used to be simpler – it was mostly about confirming human identities. But our digital world has gotten much bigger and more complicated. The workforce is no longer just human users – employees, contractors, and vendors – but also bots or service accounts, all with their own set of access requirements, restrictions, and locations.

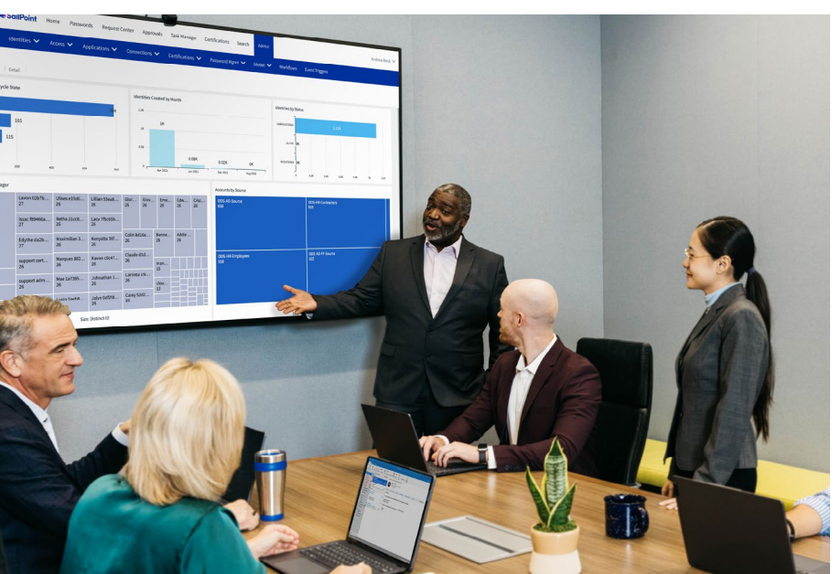
Adding to the complication, data and applications have exploded in number, spread across cloud, on-premises, and hybrid infrastructures, and often must be accessed from anywhere, on a variety of devices. This requires organizations to deliver and govern access to critical data and applications in real-time, all the time. When you do the math on the intersection of identities, applications, roles, and permissions – the numbers get really big, really fast. The results are an identity landscape that's too complicated



for humans to manage alone.

The risks are numerous and can be detrimental, including over-provisioning – giving access to those who shouldn't have it. But the biggest danger is what can result if accounts are compromised or are the target of insider or external threats: catastrophic data breaches and costly compliance violations.

Many organizations still rely on rudimentary identity tools designed to quickly authenticate and federate access. In doing so, they risk doling out access without proper governance oversight and enforcement. While tools like Identity Access Management (IAM) may offer critical lifecycle management capabilities to enable access provisioning,



they lack the risk perspective to ensure access is allocated based on approved policies and conditions, leaving other tools and procedures to step in and fill the gap. The result can be a sprawling web of confusing, disparate, disconnected systems that are anything but simple and were never designed to work together.

Unified Identity Security: A Holistic Approach

Nobody longs for Kepler's simplicity and unity more than the enterprise CISO.

At SailPoint, we call it unified identity security. Unified identity security transcends traditional IAM by providing holistic visibility, oversight, and security for the entire landscape of enterprise identities and their access. It unifies identity security controls across the WHO (every type of identity) and WHAT (all critical data and applications) to best address the needs of the complex, fast-moving, ever-evolving enterprise. This is crucial for removing siloed identity management practices and shutting down pockets of hidden risk.

Recent high-profile compromises show us that today's attackers often don't break in – they don't need to. They simply log in. That's why we at SailPoint have been leading the identity security evolution with three critical elements at our core.

1. Intelligence which provides valuable insights for pinpointing access similarities and outliers to minimize risk.
2. Automation that streamlines your identity security processes allowing you to focus on securing your organization while increasing productivity.
3. Integration that plugs-in to a wider ecosystem alongside other security tools – SSO, SIEM, XDR, EDR – offering not only breadth but depth of account, access, and activity information.

We equip the modern enterprise to manage and secure all access to applications and data across your entire IT infrastructure, ensuring just the right amount of access at the right time for all identities. We bring a simplified and unified solution to solve a complex problem. Identity security isn't just one component of your enterprise security orbit, it's the center of your solar system.

In cyber, just like in astronomy, sometimes we need to chase the new shiny objects. It's how we discover and grow. But even though Kepler watched comets and eclipses and all the wonders of the sky, it was his unifying three laws of planetary motion that simplified our understanding of the cosmos and serve as the foundation for so much of what we know today. We should enjoy and explore the comets and eclipses of our cyber world, but we can't ignore the foundational elements like identity. Security without identity is like a solar system without a sun. And what's more essential than that?

FEATURE

Downtime Cost of Cyberattacks and How to Reduce It

Cyberattacks wreak havoc across organizations. But the costs of downtime are under-discussed. How do we quantify and correct them?

By Richard Pallardy

The rise in cyberattacks has resulted in a seemingly endless litany of problems across all business types. Some of these problems are easily quantified but many are not. In the latter category, the costs of downtime stand out. Not only do cyberattacks take security analysts away from productive work and force them to deal with exigent problems, but they also disrupt the work of other professionals who rely on technological infrastructure to execute their jobs.

But it has proven difficult to assess the costs of downtime in a consistent manner. The academic literature on the subject is somewhat scant, so we must rely on reports from private businesses – that are understandably reluctant to share the financial impacts of these events unless required to do so. As a result, the figures are all over the board, varying according to industry type, length of downtime, and a suite of other factors.

What we do know is that these attacks are unlikely to abate anytime soon. Roughly 50% of organizations experienced more than 24 hours of downtime between 2014 and 2019. And large organizations are far from the only targets. Small and medium-sized businesses (SMBs) are increasingly on the radar of cyberattackers as well. Healthcare and non-finance type businesses have suffered more than three quarters of the brunt of this onslaught.

More than 80% of manufacturing companies have reported downtime in the previous three years according to a 2023 report, for example. But other types of organizations are hardly immune – over 40% of companies that use cloud services are seeing four types of attacks on the applications used to run their businesses on a weekly basis.

What Constitutes Downtime and What Causes It?

The definition of downtime is somewhat ambiguous. Generally, it refers to any time not spent on productive work

as a result of a cyberattack – by both cyber analysts and other members of an organization. Thus, it can extend to nearly every aspect of operation. Some 78% of organizations report breaches as the main source of downtime.

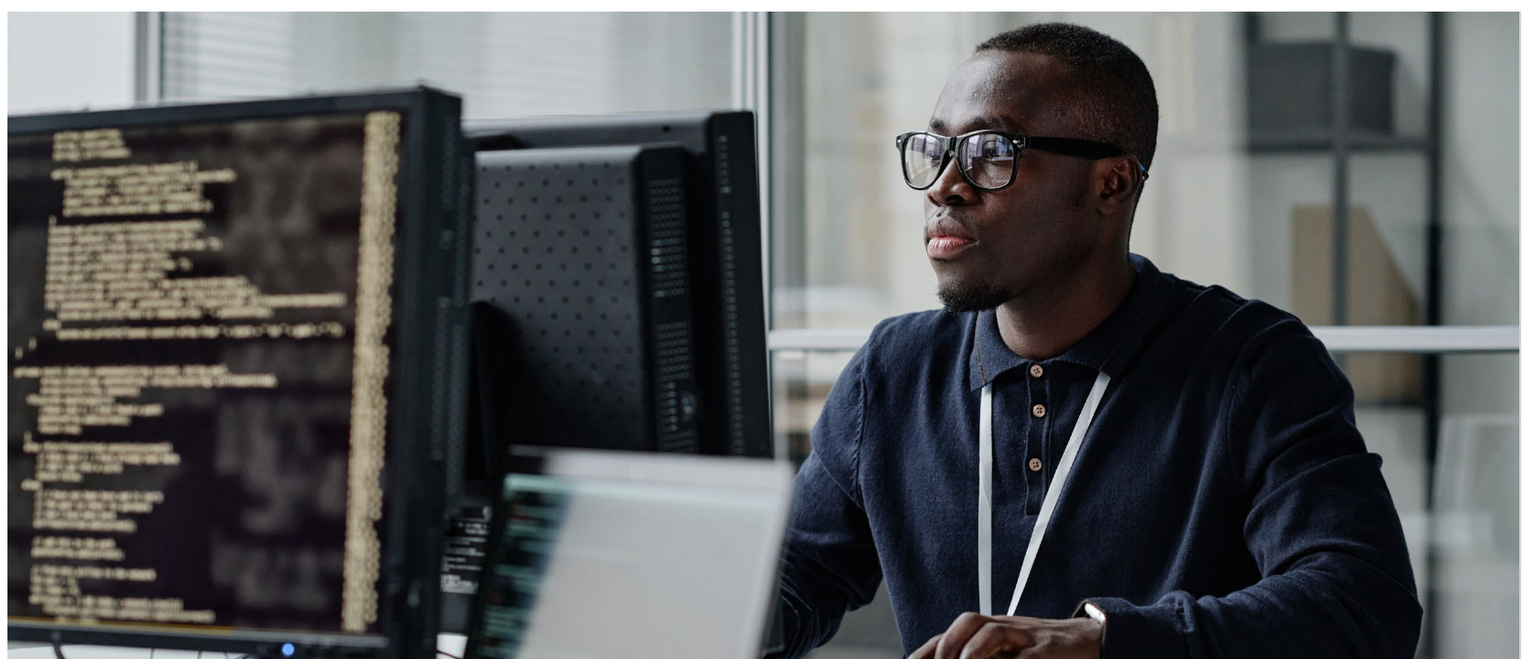
However, sometimes downtime is also scheduled for maintenance or training purposes and may occur as the result of internal errors, power outages or disasters. It may also include time spent repairing systems and equipment that have failed on their own, either due to poor planning or to unforeseen circumstances.

For cybersecurity analysts, downtime includes time spent assessing the cause of a breach, containing the breach and recovering from its effects. According to incident management software company Blameless, responding to a single incident, even a minor one, may take up to eight hours.

For other professionals, it includes lost time managing operations, contacting clients and making sales, planning for future business, manufacturing goods and any number of other tasks that lead to profitable business enabled by smoothly functioning, secure technology. Regular business may grind to a halt if, for example, a payment system or software used to guide production are compromised. Cincinnati Crane and Hoist, a small crane manufacturer, was severely impacted by a spearfishing campaign that targeted their email and payment system in 2017, for example, losing a quarter of a million dollars in revenue and resulting in the company scrambling to save its operations rather than spending time on producing equipment. Production at Molson Coors, a prominent American brewery, ground to a halt for weeks in 2021 following a cyberattack.

Downtime is sometimes unpreventable, as in the case of power outages or natural disasters. But when downtime occurs due to a cybersecurity breach, it is typically attributable to failed cybersecurity procedures and deficient business continuity plans. Even very basic cybersecurity training for employees can help reduce the likelihood of falling for common tactics such as phishing scams. So too, failure to implement a business continuity plan that establishes back-up procedures can result in companies scrambling when an event occurs. Just over half of companies have a disaster recovery plan in place according to one 2021 survey.

"Of course, staff are diverted to focus on the immediate issue, but often the first question is where exactly is the attack happening, and what exactly is impacted? Being able to observe – with confidence – the answers can help speed up response, not only by quarantining and remediating but



also by guiding decisions on whether or where to proactively shut any systems down," says Michael Dickman, chief product officer at Gigamon, emphasizing the importance of preparing for such events.

Average Costs of Downtime

The costs of downtime are difficult to estimate in a general sense. They are highly specific to business types and how reliant they are on digital systems. And there is no standard means of assessing these costs.

Below is a table of downtime cost estimates from various sources. This patchwork of data underscores the need for more extensive information sharing among industries and deeper academic work on the issue:

YEAR	INDUSTRY	REPORT TITLE	COST PER MINUTE	CYBERSECURITY RELATED
2005	Automobile	Untitled	$22,000	No
2014	[General]	Untitled	$5,600	Yes
2016	Manufacturing	Maintaining Virtual System Uptime in Today's Transforming IT Infrastructure	$4,333	Yes
2016	[General]	Cost of Data Center Outages	$9,000	Yes
2017	[General]	State of IT Management Survey	$8,662	Yes
2022	[General]	Data Protection Trends Report	$1,467	Yes

Other staggering statistics have emerged: Some estimate that manufacturers lose $50 billion a year due to downtime. If even a fraction of that cost is due to cybersecurity breaches, clearly greater consideration ought to be given to downtime planning specific to hacking incidents.

Costs range across all aspects of the business, from manufacture and sales of products to lost administrative time to effort spent tracking down new clients and new employees to replace those who fled during the chaos. And stressed organizations whose cybersecurity staff are occupied with one crisis may be vulnerable to further attacks – leading to additional downtime.

What Downtime Looks Like on the Ground

During periods of stability, cybersecurity analysts are on the offensive.

"There are different ways to categorize an analyst's time. In this context, we can think about time spent on active protection, proactive security preparation, and reactive response and remediation. 'An ounce of prevention is worth a pound of cure' is true in cybersecurity, so proactive initiatives are critical for the success and sustainability of a cyber program," Dickman says.

When they are on the defensive in the wake of an attack, these responsibilities become secondary. Work on building defenses against potential attacks is suspended – that is, if

a dedicated team is not available to man the ramparts while others head to the battlefield.

"Responding to cyberattacks is different from most other incidents. Time matters. Like any critical response team, cyber teams must train not until they get it right, but until they can't get it wrong," says Corey Hynes, executive chairman and cofounder of Skillable, a cybersecurity training platform. "The tools, procedures, and practices employed when an attack occurs have to become akin to muscle memory."

Other departments will be similarly distracted from their typical duties. Customer service representatives will be diverted from fielding everyday complaints and inquiries to doing damage control for hordes of unhappy customers. Finance professionals will be pulled from their bookkeeping duties and asked to investigate potentially compromised customer accounts. Public relations officials will turn from promoting the company to stanching the reputational damage that usually occurs when breaches become public. And the C-suite will pivot from making deals and managing operations to reassuring client representatives and board members.

The Parable of Hospital Downtime

Downtime in hospitals is among the better studied scenarios in the academic literature. Many hospitals are also research institutions, and the cost of downtime is not just financial – it can result in healthcare consequences, even lost lives. Further, hospitals are prime targets for cyberattackers, with some 166 hospitals attacked between 2012 and 2018 alone, resulting in an estimated 701 days of downtime. Healthcare institutions are thus incentivized to share their messy, ad hoc procedures – and the lessons they learned from them – in ways that some private industries are not.

Due to their heavy reliance on digital recordkeeping, these organizations must devise radically different means of communication if those systems are affected by an attack. Even when outages are not complete, they may pose a danger to patients. For example, if clinical decision support mechanisms in electronic health care records are compromised, treatments that might otherwise be flagged as potentially dangerous are implemented anyway.

As the digital generation comes of age and enters the working world, many professionals are unfamiliar with paper record keeping and non-digital means of communication, presenting an added challenge in devising downtime procedures. During one outage, physicians had to hand-write prescriptions and may have compromised patient safety due to their lack of familiarity with how to correctly indicate drugs and dosages.

Developing templates in case of such outages will likely be useful. One hospital pathology lab did so on the fly following an attack, which proved helpful, but the approach would have been more efficient if prepared ahead of time. Staffing had to be doubled to implement the approach, another consideration for downtime planning extending to budgeting and staff management.

> **"Responding to cyber-attacks is different from most other incidents. Time matters."**
>
> – Corey Hynes, Executive Chairman and Cofounder of Skillable

During a 2017 downtime event at an Australian hospital due to the WannaCry attack, staff used a combination of email, text messaging, in-person meetings, paper records and public announcements via the loudspeaker system.

"Familiarity with medications and all of the things that are associated with clinical care is just so much easier with the electronic record and people become used to that. You don't realize how automated things are now with the electronic record and the checking and all those things that go on within the record [that] are not available in the paper system," one of the staff members interviewed by the researchers said.

While staffers were initially hesitant to use the PA system due to fears of disturbing patients and their families, announcements turned out to be key to ensuring smooth communication. In person meetings were thought by most interview subjects to be the most effective means of transmitting information. However, other research emphasizes that written communication is essential – verbal directives cannot always be verified due to the busy nature of the hospital system. Text messages protocols, runners to transfer paperwork, and even the use of large white boards have been used to ensure the accurate transmission of information.

How to Plan for and Deal With Downtime

Having some form of business continuity and disaster recovery (BCDR) plan in place is probably the best prophylactic against major downtime costs. More than 90% of managed service providers report that such plans are likely to reduce downtime according to one report. A study of healthcare providers indicates that incident response plans may reduce downtime by as much as 48% a month.

"Your systems exist in a continuous state of partial degradation, and you are positively swimming in failures," notes Charity Majors, chief technology officer and cofounder of Honeycomb. All eventualities, from minor disruptions to full shutdowns, need to be planned for if downtime is to be used efficiently.

"IT leaders and other business decision makers must think critically about their support teams, identifying and encouraging continual upskilling via real-world scenarios to mirror the threats they're likely to experience," Hynes advises. "Staying skilled in parallel to increasingly complex and intelligent cyberattacks can make recovery more efficient and alleviate unnecessary downtime that puts the company reputation and stakeholder relationships at risk."

This will often necessitate de-siloing an organization. As one paper observes, cybersecurity analysts are sometimes not looped into continuity plans, making those plans next to worthless when something actually happens. Conversely, analysts do not necessarily share the findings of their risk assessments with the necessary departments. So, nobody can plan accordingly.

As previously referenced, planning for alternate means of communication, whether it be in a hospital or in another business, is crucial. Ensuring that an immediate fallback to typical communication channels is in place will almost assuredly save time in the event of an attack.

Once plans are in place, they need to be tested to assess potential weaknesses. But planned downtime is a luxury most organizations can no longer afford, Majors says.

"Once upon a time, we had 'planned downtimes' – we'd take the system offline for a night while we repaired a drive or repointed the primary," she recalls. "Nobody thinks this is acceptable anymore. The frequency and duration of our total

outages have been steadily dropping for years. But this doesn't mean things don't break."

"As the saying goes, 'If it hurts, do it more.' If it hurts, and is hard, and takes a long time to deploy some code, you should do it again and again and again until it's fast and easy," she adds. "When it comes to software, speed is safety, much like riding a bike or ice skating. Anything that gets done every day will be easy and effortless. Anything that you do only once a year under extreme duress is going to hurt like hell."

Procedures for securing the environment following an attack need to be put into place as well to ensure that downtime is not wasted during recovery – it will be useless if another attack is just over the horizon.

The National Institute of Standards and Technology provides useful guidance with its Cybersecurity Framework. Of the five categories, identify, protect, detect, respond, and recover, Dickman says some are overlooked.

"Identify, detect, and recover have too often been neglected, which makes protect less successful, and respond slower and less complete. One important improvement that helps all five of these functions is creating the infrastructure ahead of time to observe the movement of data and the interactions of users and applications, in a way that is immutable and complete," he claims. "Having this kind of deep observability will Identify threats faster, inform better protection policies, detect a greater proportion of threats, focus response faster and in the right place, and give confidence that recovery is safe and successful."

How to Build True Cyber Resilience

It isn't possible to stop every attack, but how can organizations embrace a resilient cybersecurity posture?

By Carrie Pallardy

Hackers will find a way in. The inevitability of a cyberattack can be a tough pill to swallow. But once leadership teams accept that not every attack can be thwarted, they can prepare their organizations to respond and recover effectively. The concept of cyber resilience is much discussed, but it takes time, resources, and organization-wide commitment to achieve.

Defining True Cyber Resilience

Cyber resilience is a business objective, according to Richard Seiersen, chief risk officer at IT services and consulting company Resilience. "Resilience comes down to the ability to continuously deliver value to your stakeholders, even when facing material losses," he explains.

Organizations need a shift in mindset and security strategy to achieve this business objective. First, leadership teams need to acknowledge that cyberattacks are inevitable. From there, they can assess the risks specific to their business, build the strategies necessary to mitigate those risks, respond when an attack does happen, and continue operations while working through an incident.

Cyber Resilience Today

Where are organizations in their journeys to cyber resilience today?

Cybersecurity awareness has grown in recent years. It is no longer just an IT and security executive concern. The rest of the C-suite and board members are getting onboard, but understanding the need to recognize and respond to cyber threats is just the first step to actually implementing cyber resilience.

"I think most organizations understand that they will be attacked at some point, so in theory they understand the need for a focus on cyber resilience; but they are struggling to implement and measure it as a program," says Tia Hopkins, chief cyber resilience officer and field CTO at managed detection and response company eSentire.

Seiersen considers risk mitigation, transfer, and

acceptance as core elements of cyber resilience. “I believe most companies do some components of cyber resilience,” he shares. “They buy insurance (transfer), security controls (mitigation), and have capital reserves (acceptance). But the groups that do each of these activities work in isolation, each working towards their own objectives.”

Cyber resilience is a holistic concept, and a fragmented approach makes it difficult to achieve. It may be particularly challenging for smaller organizations to move away from that fragmented approach.

“Cyber resilience these days is the privilege of mainly larger organizations. Small and medium size enterprises opt-out to fragmented cyber defense and often don’t have access to cyber and business continuity experts that can formulate a meaningful path for better cyber resilience,” says David Chernitzky, CEO of cybersecurity company Armour Cybersecurity.

But there are signs of progress. For example, organizations are cutting down the time that it takes to respond to threats. The Cyber Workforce Benchmark report from of cybersecurity skills training company Immersive Labs found that organizations’ response time went down from 29 days in 2021 to 19 days in 2022.

James Hadley, CEO and founder of Immersive Labs, believes that faster response times are a positive sign; faster response times mean organizations are addressing vulnerabilities and reducing the risk of negative impact.

While there is no shortage of headlines and research that underscores the importance of cyber resilience, it may take a real-life incident to galvanize leadership teams to action.

“Only a small number of organizations are proactive in building their cyber resilience; the majority of organizations I’ve met throughout my career had to go through unpleasant experiences of cyber incidents to start their journey to a more cyber resilient future,” says Chernitzky.

Building a Strategy

Cyber resilience cannot be achieved by implementing one initiative or investing in one new technology. “CISOs should focus on the question, ‘How ready are we?’” says Hopkins.

Are organizations ready to detect threats, respond to them, recover, and adapt to an ever-changing threat landscape?

"The first step to building cyber resilience involves understanding which cyberattacks are most relevant to an organization based on its industry, location, IT ecosystem, data type, users, et cetera," says Tony Velleca, CISO at digital technology and IT service company UST and CEO of CyberProof, a UST security services company.

Once an organization understands its risks, the question becomes how to detect those threats, stop them, and contain them if and when they become cybersecurity incidents. The answer lies in a blend of technology and talent.

Combining the power of cybersecurity tools, such as zero trust and managed detection and response, can help organizations achieve cyber resilience, but they need to ensure the strategies they deploy make measurable progress toward that goal.

"Organizations can no longer rationalize investing in costly traditional cybersecurity training, nor can they dump all their money into tech stacks alone," Hadley cautions.

Instead of taking a check-the-box approach to cybersecurity, Hadley encourages regular cybersecurity exercises and hands-on labs that give actual metrics that reflect a team's abilities to respond to incidents.

"Take an always-on approach that consists of regular exercising and obtaining measurable improvements, which will ultimately lead to stronger cyber postures for the organization and instill the needed confidence to know

teams are actually ready when a crisis hits," he says.

Leadership also needs to consider where their data lives and the kind of talent necessary to keep up with an evolving threat landscape. Many organizations have migrated from data centers to the public cloud or are in the process of doing so.

"A key problem for enterprises undergoing cloud migration is human resources. Your existing cybersecurity team may not have prior experience with this. An enterprise needs to retrain or upskill its talent or to start finding new talent," says Velleca.

Remember that cyber resilience is not achieved and then forgotten. It requires regular updates to its strategic pillars to remain effective. Organizations can schedule regular annual, semi-annual, or quarterly reviews of cybersecurity processes, like detection and incident response. But agility is essential. Any change in an organization's environment introduces gaps and opportunities for threat actors to exploit.

"There are events such as security incidents, infrastructure changes, cloud adoption, mergers and acquisitions, office relocation, major industry breaches – the list goes on and on – that should be considered triggers for review outside the regular cadence," says Hopkins.

Budgeting for Cyber Resilience

Recovery is essential to cyber resilience, but spending in many organizations is skewed toward defense. InformationWeek surveyed 180 IT and cybersecurity professionals in the Cyber Risk and Resiliency Report: How CIOs Are Dueling Disaster in 2023 and found that company spending, on average, is 70% on defense and 30% on recovery.

Leadership teams likely need to reevaluate cybersecurity spending to determine how to fund a resilient strategy effectively. The answer isn't abandoning defense and pouring money solely into response. It is about finding a balance that works for an organization.

"Cyber resilience is a much more holistic concept, balancing

investments in mitigation, transfer, and acceptance to ensure the business is able to fulfill its mission – particularly when facing material losses," says Seiersen.

Hopkins cautions against using fear, uncertainty, and doubt as a means to persuade board members and senior leaders of the importance of cyber resilience. "Decision-makers may not respond well because they might struggle to connect the dots between what's going on in the threat landscape and the financial impact to the business," she says.

Instead, CISOs and other cybersecurity leaders can use the art of storytelling to effectively communicate with other leaders and board members.

"Education and storytelling about how cyber can cause much pain to an organization enable CISOs and CIOs to be successful in getting buy-in from stakeholders and appropriate budgets for cyber resilience," says Chernitzky.

The Future of Cyber Resilience

As companies grapple with the realities of the threat landscape, cyber resilience will likely be adopted out of necessity. Additionally, new regulations could have a hand in driving this trend. Seiersen offers the new Securities and Exchange Commission (SEC) rules on cybersecurity as an example. In July, the SEC announced new rules that will require public companies to report material cybersecurity incidents.

"I think the new SEC cyber rules will be a forcing function for businesses to focus on material losses over generalized cybersecurity, and it will soon become the de facto approach," says Seiersen.

The changes cyber resilience drives in cybersecurity culture could be reflected in the C-suite. "We'll continue to see the cyber resilience function, whether as a standalone C-level position or as part of the CISO or CSO role, officially take shape within organizations," Hopkins expects.

Organizations that want to achieve cyber resilience will need to commit to implementing a holistic strategy and continuous skill improvement for all team members.

"Hopefully, in three to five years, we will see many more organizations that can withstand cyber-attacks that would destroy them today," says Chernitzky.