aftra.io

aftra

Management's Guide to Cybersecurity

Navigating your business from data risk to data security

Contents

Key takeaways

By the end of this paper, you'll be armed with the knowledge you need to act on the following areas:

1. **Understand your vulnerabilities:** As your company digitizes more assets like email, web apps, databases, hosted services (such as databases, FTP servers, web servers, IoT services, etc.)… these all expand the potential attack surface and risks for cyber threats.

2. **Proactively assess and shrink attack areas:** Continuously discover and evaluate vulnerabilities in your external attack surfaces, then prioritize and mitigate the most urgent threats, while taking steps to shrink your attack surface.

3. **Developing an incident response plan:** Only 15% of companies have a mature incident response plan today. Make sure your company documents protocols, implements monitoring for early warning signs, and is prepared to take action.

4. **How to involve leadership and align with tech leaders:** Boards and executives need to understand cyber risks and strategy. Collaboration with CTOs on regular evaluations, benchmarks and improving security is key.

Introduction

Think of all the parts that allow your business to operate digitally as pieces of a growing city.

Domain names form street addresses, servers act as buildings that house data, and customers are citizens accessing services.

As your digital enterprise expands, unseen gaps and hazards also multiply. Cybercrime lurks around every virtual corner, from viruses disrupting operations to data thieves stealing customer records. One overlooked flaw can leave the entire digital town exposed.

As mayor of this virtual city, the buck stops with you if a crisis strikes. And, we hate to say, it’s rarely an “if” but a “when”. That’s because when it comes to cybersecurity defense, the game is stacked in favor of attackers: defenders need to get **everything** right, while hackers only need **one** vulnerability.

The expansion of attack surfaces in a post-pandemic hybrid world, combined with shrinking teams and budgets and the rapid rise of generative AI, are fuelling a growing need for companies to ramp up their security posture.

Currently, spending on security tools is not proportionate to the potential cost of a breach.

The average incident now costs businesses a jaw-dropping $3.86 million. Yet, on average, companies allocate less than 10% of IT budgets for protection. Luckily, when cracks emerge in the pavement, external eyes can quickly pinpoint potholes before they crater into sinkholes.

This means it’s never been more important to scan the expanse beyond your internal firewall border, monitoring external threats you can’t see. You need a neighborhood watch for your digital domain, a lifeguard at your public data pools.

This guide explores unseen dangers poised to disrupt businesses and how Aftra checks blind spots. It’s time to safeguard all the important, dedicated employees and digital assets that make your hard-working business operate successfully. After all, the digital streets move fast.

> **“The Board of Directors’ responsibility is to make sure that the executive team has a plan, is prepared, and is preparing the whole organization for the eventuality of an attack.”**
> ***– Wolf Richter, CIO Counsellor, McKinsey***

Grasping your external digital exposure

Let's survey your digital city's outer districts – rarely patrolled terrain where hazards multiply if they're unchecked.

First up, we need to understand the sheer breadth of assets indirectly under management's guardianship.

When we say "the external attack surface", we're talking about all parts of an organization's IT infrastructure linked to the public internet. So that means employee email, customer-facing web applications, exposed databases, file storage buckets accessible anonymously online – essentially any technology visible externally.

> **Only 1% of companies are fully aware of their internet-facing assets**
> *– Gartner*

Your external attack surface

- Employee email environments
- Customer facing web applications
- Exposed databases and data lakes
- Network adjacent cloud assets and tools
- Hosted services (such as databases, FTP servers, web servers, IoT services)

Outdated software no longer maintained, orphaned cloud resources lingering forgetfully - what do you get? Increased risks. Retired platforms with concluded lifecycles, former employee tools removed from inventory lists, leftover merger-and-acquisition artifacts… they all need governing to avoid becoming hacker havens.

Careless configuration management is also guilty of granting unnecessary access. Something as simple as an over-permissioned cloud storage service with public visibility, rather than locked down for specific users, offers tempting, low-hanging fruit for data thieves.

On the same note, failing to use multifactor authentication to confirm employee identities before granting access to sensitive documents provides a foothold for impersonators. Neglecting to timely patch published software vulnerabilities is basically offering up another candy store of exploitable technical oversights.

Shining a light across your digital shadow

The list of seemingly small missteps adding up to gigantic risk continuously expands as infrastructure sprawls globally.

Maintaining ongoing visibility then rapidly shrinking these holes remains crucial.

This includes governance of shadow IT (digital tools created or downloaded outside company tech policies) from unauthorized tools that evade oversight - but pose data leakage - and operational disruption dangers if exploited.

External attack surface management (EASM) brings focus, expanding visibility to enable security and IT teams to govern known risks.

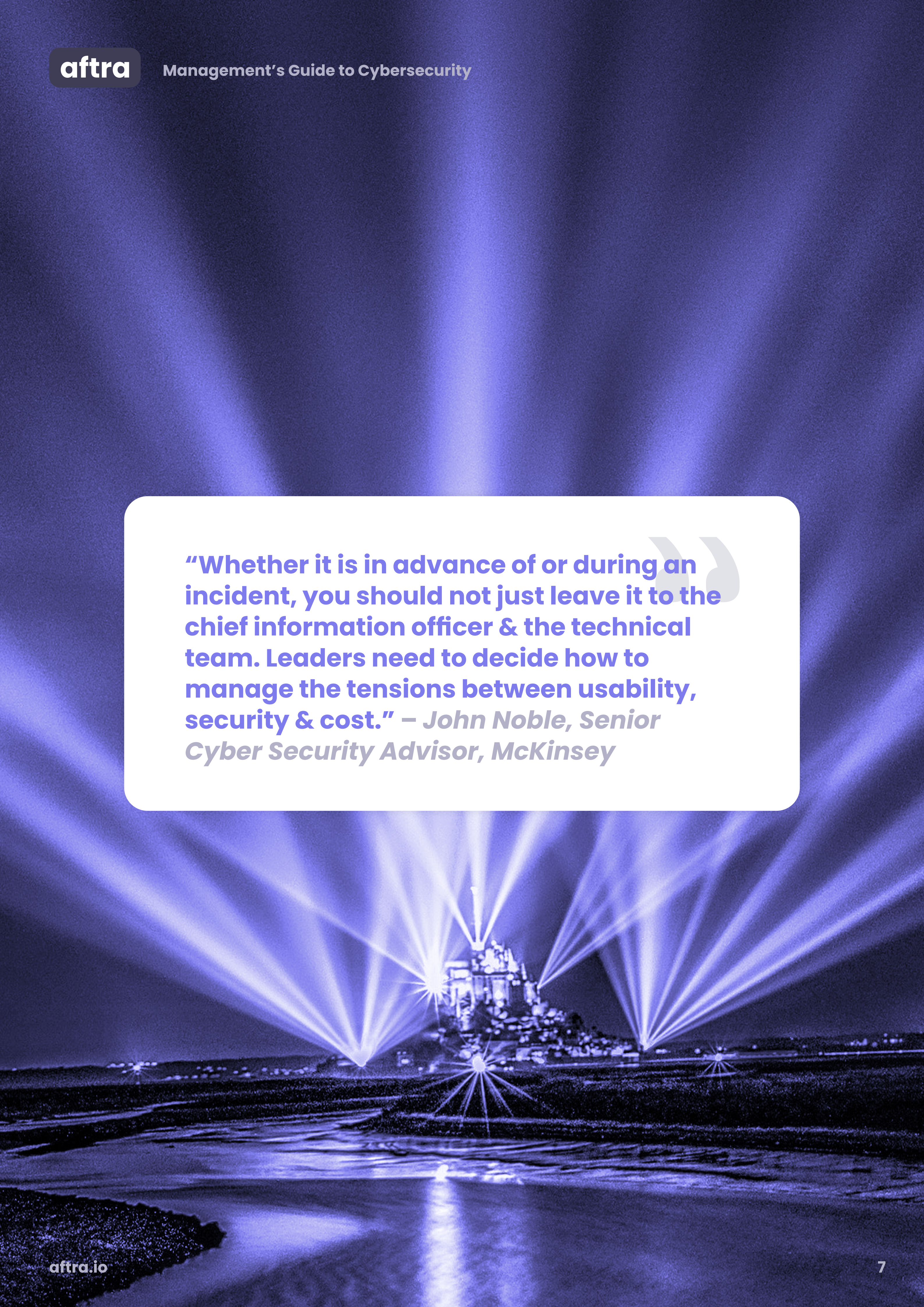
> **Less than 10% of organizations have adopted one or more attack surface monitoring technologies to address their attack surface** – *Gartner*

How EASM works:

- **Discovery:** Identify and list all external assets
- **Enumeration:** Gather details and profile each asset
- **Vulnerability management:** Scan for weaknesses and prioritize risks
- **Risk mitigation:** Develop a plan and implement security measures
- **Continuous monitoring:** Establish ongoing monitoring and adapt to changes

Fortifying defenses all begins with comprehensively identifying assets across on-premise data centers as well as among complex multi-cloud architectures. Discovery uncovers the entirety of technology upkeep that teams must continually monitor and secure.

Aftra's differentiated value lies in illuminating the full breadth of an organization's external-facing digital footprint - automatically discovering assets, access points and vulnerabilities that overextended security teams often overlook. Neglecting to timely patch published software vulnerabilities is basically offering up another candy store of exploitable technical oversights.



“Whether it is in advance of or during an incident, you should not just leave it to the chief information officer & the technical team. Leaders need to decide how to manage the tensions between usability, security & cost.” *– John Noble, Senior Cyber Security Advisor, McKinsey*

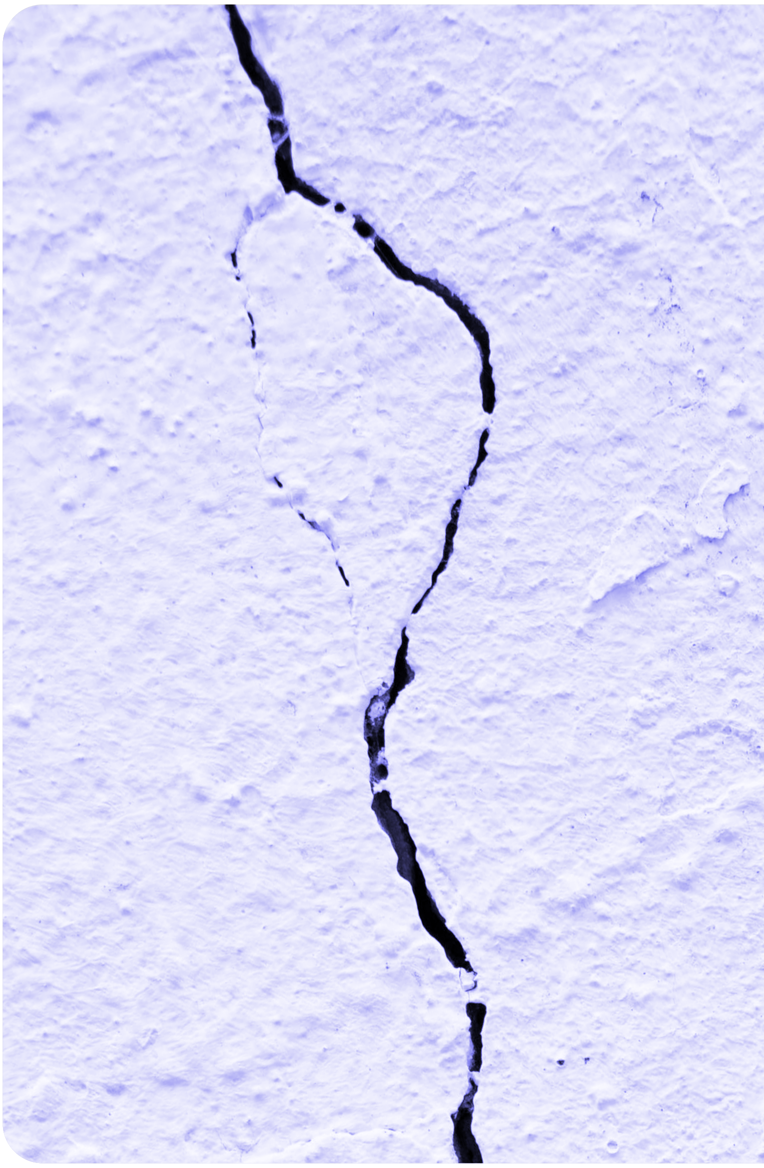
Pinpointing your security shortcomings

Keeping up securing rapidly-expanding digital systems can often become overwhelming without consistency and automation. Gaps continuously emerge as environments quickly scale - meaning small oversights accumulate into major incidents.

Let's look at how small insights can escalate:

- **Example:**
  Neglecting timely application of critical software updates
- **Exploitation:**
  Cybercriminals exploit unpatched vulnerabilities
- **Privilege escalation:**
  Attackers escalate privileges, gaining control
- **Data breach/disruption:**
  Results in data breach or system disruption
- **Reputation & legal impact:**
  Damage to reputation, legal consequences and financial losses
- **Regulatory non-compliance:**
  Potential regulatory compliance issues arise

To prevent these kinds of incidents, EASM software plays a crucial role in addressing security gaps and pinpointing shortcomings. It provides a proactive approach to cybersecurity by continuously monitoring and managing an organization's external attack surface.



How EASM helps:

Comparing to security benchmarks:
EASM software assesses an organization's security measures against established best practices and industry benchmarks. This involves comparing configurations, policies and practices against recognized standards to determine adherence and identify deviations.

Identifying gaps in architecture:
Through automated scans and checks, EASM software identifies gaps in the organization's architecture. This includes vulnerabilities, misconfigurations or areas where security practices deviate from established benchmarks.

Automated policy checks for gaps:
EASM performs automated policy checks across various domains, including cloud configurations, network settings and web assets. It systematically evaluates these against best practice frameworks to ensure compliance and security.

Assessing configurations:
The software assesses configurations related to cloud infrastructure, network settings and web assets. It analyzes these configurations to identify potential weaknesses that could be exploited by attackers.

Prioritized opportunities for improvement:
After identifying gaps, EASM prioritizes them based on potential business impact. This prioritization enables organizations to focus their resources on fixing the most critical issues first.

In a nutshell, EASM acts as a roadmap for gradually addressing gaps, despite exponentially growing technology footprints.

How Equifax learned the hard way

The Equifax data breach in March 2017 impacted over 140 million Americans and exposed highly sensitive personal information. An unpatched Apache Struts vulnerability allowed initial access for hackers. Poor security practices then enabled attackers to easily move through Equifax's systems undetected for over two months.

Key issues that enabled the breach include:

- Failure to patch a known vulnerability
- Lack of network segmentation allowing lateral movement
- An expired encryption certificate masking data exfiltration
- Plaintext storage of passwords further opening access

The data has not appeared on the dark web leading investigators to believe Chinese state-sponsored hackers carried out the attack for espionage.

Fallout for Equifax included:

- Over $1.4 billion spent on upgraded security
- $1.38 billion settlement with the FTC
- Executive departures and credit rating downgrade

Six years on from the breach, Equifax is still paying for the incident – in October 2023, UK watching Financial Conduct Authority fined the company a further $13.4 million.

Monitoring for emerging threats

Gaining visibility into risks targeting your organization means faster preparation before incidents strike. Early warning threat indicators should be a key priority for security-conscious businesses.

Continuous threat monitoring creates an essential smoke alarm system for potential cyber attacks, empowering teams to accelerate incident response.

Leading types of threats:

Ransomware: Persistent threat causing widespread disruption and financial harm through file encryption and ransom demands.

Phishing attacks: Deceptive tactics targeting individuals for sensitive information compromise, posing significant cybersecurity risks.

Credential compromise: Unauthorized access through stolen or weak credentials remains a prevalent and damaging threat.

Zero-day exploits: Attacks exploiting undisclosed vulnerabilities demand proactive defenses to counter emerging risks.

Distributed Denial of Service (DDoS) Attacks: Growing in scale and sophistication, distributed denial of service attacks pose a serious threat to online services, requiring robust mitigation strategies.

Advanced persistent threats (APTs): Stealthy and prolonged cyberattacks by skilled adversaries necessitate advanced detection and response capabilities to safeguard critical assets.

Early warning threat indicators play a crucial role in proactive cybersecurity by providing timely insights into potential vulnerabilities, malicious activities, or changes in the external attack surface.

A cybersecurity risk assessment tool's indicators may include:

- Unusual network activity
- Changes in asset configurations
- Alerts from threat feeds
- Suspicious user behavior
- Unusual access patterns
- Security event logs
- Phishing indicators

Aftra partners with security research firms to deliver contextual threat intelligence tailored to our customers' environments. This includes monitoring activity on underground hacker forums and the dark web which can provide early warning around emerging campaigns targeting key assets.

Additional priority indicators track exploits weaponizing vulnerabilities in popular SaaS applications like Office 365 and cloud platforms. Integrations with firewall, endpoint detection and other monitoring tools analyze signals from these security layers to enrich awareness and provide multiple perspectives identifying risks.

Why Uber keeps getting attacked

Uber was breached yet again in January 2023 via a third-party vendor - Genova Burns LLC, a law firm with access to driver records. Over 77,000 Uber and UberEats drivers had personal data stolen, including names and social security numbers.

This latest incident marks Uber's third breach in six months, sparking renewed scrutiny of their security posture. As experts note:

- Uber's "traditional approach" to cybersecurity is not cutting it
- Need for end-to-end security versus a siloed view
- Minimizing vulnerabilities from third-party access and partnerships
- Improving human-centered behavioral factors, not just technical controls.

The breach augments existing criticism of Uber's history of lapses:

2022:
Hacker gains internal system access "for fun"

2016:
57 million customer and driver records breached, then allegedly concealed

The consensus among experts is that Uber must shore up both technical and human vulnerabilities across their ecosystem of access now that drivers' sensitive personal information is yet again compromised.

Activating incident response

When threats emerge, swift yet methodical response bridges detection to resilience. But remember: prevention is equally crucial in the cybersecurity landscape. Organizations must prioritize preventive measures, such as ongoing assessment and reduction of the attack surface, to minimize the likelihood and impact of cyber incidents.

> **Just 15% of organizations globally are deemed to have a mature level of preparedness to handle the security risks of our hybrid world** – *Cisco*

- **Document:** Create plans for responding to common threats like ransomware or credential theft. Specify how to fix misconfigured assets based on their criticality.
- **Build:** Run simulations and workshops to understand the impact of cyberattacks. Learn from incidents, improving playbooks to prevent similar issues.
- **Track:** Use centralized dashboards to assign and track tasks. Include features like comments and due dates for accountability.
- **Quantify:** Measure risk reduction over time. Communicate program maturity to justify increased investments.Learn from incidents, improving playbooks to prevent similar issues.
- **Scale:** Move beyond reactive measures. Continuous visibility and automated systems help identify threats early, sustaining security gains.

Aftra combines these practices – prescriptive, plan-language recommendations, coordinated workflow and progress measurement – enabling resilience at scale.

How slow response time was JBS' downfall

In May 2021, a ransomware attack on meat processing giant JBS disrupted operations globally until an $11 million ransom was paid.

JBS had rampant malware and was "extremely slow" to address vulnerabilities - a worrying sign as food production constitutes critical infrastructure. The large attack surface, lack of segmentation and prevalence of outdated systems create inherent Industry weaknesses ripe for exploitation.

Post-attack, the FBI warned the sector of increased targeting. Breaches occur daily but rarely become public. JBS highlights the need for basic security hygiene like patching and upgrading legacy systems.

The attack itself began months prior and progressed through common stages:

- Employee credentials leaked online
- Hackers infiltrate systems extracting data
- Ransomware activated halting operations

The JBS attack puts aging infrastructure and lax security practices in the spotlight, underscoring the critical need for modernization and resilience across the food supply chain.

Enhancing cybersecurity resilience

Inadequate security not only incurs immediate costs but also leads to long-term consequences, with customer trust and revenue continually diminishing in the aftermath of disruptions.

> **75% of consumers are willing to stop using a brand if it faces a cybersecurity problem**
> ***– Vercara***

The ramifications extend beyond immediate recovery expenses necessitating ongoing vigilance in the face of persistent adversary innovation.

Acknowledging that security challenges evolve requires a proactive approach. Continuous visibility across the entirety of attack surfaces, combined with systematic exposure reduction, fortifies your organization's security posture against emerging threats.

Proactive cybersecurity fuels resilience

Threats evolve rapidly, but resilience stems from anticipating change, not reacting to it. Continuously strengthening defenses before adversity strikes sustains operations during turbulence.

Swift yet measured responses

Early detection enables precisely contained reactions, thwarting incident escalation. But resilience requires response devoid of impulsiveness, as methodical mobilization minimizes collateral disruption.

Shrink danger zones

Regularly consolidating control areas limits adversary maneuverability. Reducing the cyber asset attack surface narrows opportunities for penetration by incrementally governing technology across all touchpoints.

Strategic alignment maintains trust

Vigilance communicates commitment to all stakeholders. While some incidents remain inevitable, resilience arising from anticipating change rather than reacting to it earns confidence by signaling preparations to preserve continuity should crisis strike.

Why Aftra is the future for proactive defense

Businesses face exponentially expanding digital footprints filled with overlooked gaps that malicious actors exploit. But legacy tools lack comprehensive visibility into internet-facing assets outside firewall borders operating as unchecked risk domains.

Aftra moves beyond limited internal vulnerability scanners to automatically expose threats across the external attack surface, including obscure organizations, domains, clouds and technologies facing the Wild Wild Web.

Core capabilities span:

Automated asset discovery

Continuously surfaces unknown exposed areas typically hiding in plain sight.

Configuration monitoring

Assesses settings against benchmarks immediately surfacing preventable oversights.

Prioritized improvement opportunities

Quantifies potential impact focusing limited resources on fixes delivering broadest risk reduction.

Emerging threat intelligence

Custom detections warn of indicators requiring accelerated response based on infrastructure.

Prescriptive mitigations

Plain language remediations to incrementally govern ballooning exposure.

These differentiated visibility, detection and response features shrink the terrain where adversaries operate – equipping understaffed IT and security teams to harden defenses amid dynamically scaling complexity.

Schedule a demo today to illuminate current external exposures and how Aftra immediately improves security posture through data-driven decisions.

Conclusion

As we conclude our tour of the digital metropolitan your business relies on, it's clear that unseen gaps and hazards multiply as this virtual city expands. Yet strong leaders recognize uncontrolled growth invites adversity.

With customer data and transactions flowing at an ever-quickening pace, taking a reactive approach to security ultimately leads to crisis.

Luckily, trusted guidance exists for governing sprawl before cracks become catastrophic breaches. Aftra surveys the darkest alleys and farthest-flung districts, freeing your IT first-responders from perpetual panic firefighting.

Our bird's-eye view reveals subtle vulnerabilities easily exploited by increasingly crafty digital pickpockets.

> **By 2025, cybercrime is projected to cost US$10.5 trillion in damages – a 300% increase from 2015 levels** – *McKinsey*

Aftra's proactive approach empowers you to identify and mitigate vulnerabilities across all digital assets, including cloud-centric resources, strengthening your cybersecurity posture and minimizing the risk of breaches.

By prioritizing preventive measures alongside incident response strategies, you can effectively fortify your defenses and mitigate the impact of cyber incidents on your operation and reputation. Ongoing foot patrols, coupled with measured recommendations for shrinking exposure, will pay dividends when the next attack emerges. Consider Aftra your CISO-as-a-service, equipping you to strategically fortify defenses amid adversaries operating at scale.

Next steps: Approaching your CTO

After reading this, your natural next step is to schedule an executive cybersecurity briefing to align on risk exposures, response readiness and opportunities to strategically mature defenses. Here are nine things which should be on the agenda:

1. **Understand your digital landscape:** Conduct a thorough assessment of your digital assets, including employee email, customer-facing apps, databases and cloud resources.
2. **Identify potential risks:** Govern retired platforms, orphaned resources and over-permissioned services to mitigate potential security risks.
3. **Explore external attack surface management (EASM):** Investigate EASM security solutions to gain focused visibility into your organization's external-facing digital footprint.
4. **Benchmark against best practices:** Evaluate your security measures against industry benchmarks and best practices to identify areas for improvement.
5. **Implement automated policy checks:** Introduce automated policy checks for gaps in cloud configurations, network settings and web assets to ensure compliance.
6. **Assess and prioritize improvements:** Use EASM software to assess configurations related to cloud infrastructure, network settings and web assets, prioritizing fixes based on potential business impact.
7. **Continuous threat monitoring:** Establish continuous monitoring for emerging threats, including ransomware, phishing, credential compromise and advanced persistent threats (APTs).
8. **Activate incident response plans:** Codify incident response plans for common threats like ransomware or credential theft, conduct simulations and centralize dashboards for unified tasks.
9. **Quantify risk reduction:** Measure and communicate the progress of your cybersecurity program, quantifying risk reduction over time to justify ongoing investments.

60% of CTOs believe that technology is not aligned with the business objectives in their organisation – *Deazy*

Establishing a shared baseline understanding of cyber risk empowers intelligent collaboration on minimizing operational disruption when - not if - the next incident emerges.