eBook

AVERTIUM

2023 CYBERSECURITY LANDSCAPE:

8 LESSONS FOR CYBER-SECURITY PROFESSIONALS

Dive into practical steps you can take to enhance your organization's level of cyber maturity, today.

TABLE OF CONTENTS

INTRODUCTION

LOOKING BACK, LOOKING AHEAD

Looking back, 2022 was marked by:

2022 was marked by increased investment in cybersecurity alongside increased complexity in the cybersecurity technology landscape. Bad actors took advantage of this complexity, finding novel ways to infiltrate and disrupt organizations for financial, political, or even reputational gain – and no industry was safe.

A great proportion of attacks in 2022 were laced with a distinctly human element wherein attackers exploited human error as employees increased their reliance on remote platforms. Nevertheless, in 2022, companies continued down the path of digital transformation, often failing to consider the implications of these shifts on their attack surface.

So what's ahead in 2023?

As we move into 2023, it is important to learn from the past, eliminate the weaknesses that you can, and then use the data you have to anticipate and proactively mobilize against future attacks.

Because whether attackers build upon the classic attack techniques of the past or identify novel ways of thwarting our defenses, as we move into 2023, one thing is abundantly clear: **When it comes to cybercriminals, they'll find a way.**

LESSON 1: Despite a complex landscape, tried & true tactics still work.

Despite the advancement of technology, many of the old tricks still work. For several years, the number 1 attack vector leading to breaches has been web applications. This hasn't changed. Social engineering is another one of those tried and true tactics that even the most inexperienced threat actors can be successful with.

Looking Back: New Threat Actors Utilized Classic Attack Playbooks

In 2022, many cyber attacks were executed by newer, less experienced, and less organized threat groups. But make no mistake: just because these bad actors were less sophisticated, that doesn't mean that their attacks were any less devastating.

For example, meet Lapsus$.
Lapsus$ is a hacker group composed of Gen Zers ages 16-21. Lapsus$ wasn't exactly cautious or discrete in their approach. In fact, they had an open Telegram channel where literally anyone could join their conversations. Lapsus$ didn't have sophisticated tactics and techniques either. Instead, they gained access to networks by employing tried and true tactics, like:

Recruiting former disgruntled employees that previously worked for the large companies

SIM swapping

Social engineering

Lapsus$'s fearless leader was none other than a 16-year-old who still lives with his parents – parents who were unaware that their teenager spearheaded massive attacks on global corporations like Okta, Microsoft, Ubisoft, and Samsung.

Related Content: *Lapsus$: An In-Depth Look at the Data Extortion Group*

The takeaway here is that the barrier to entry for a cybercriminal in today's threat landscape is very low. Threats are anywhere, and they can be deployed with minimal effort.

Looking Ahead: Don't Ignore the Basics

Classic attack techniques are not going away. And yet, companies are still failing to cover many of the basic attack vectors attackers use.

The good news?

Companies at all levels of maturity can shore up their defenses to protect themselves against these threats. Organizations need to tighten up security basics: we don't always need to be caught up in the latest 'silver bullet' or 'high speed' tool. *If you're putting lasers in the air vent but leaving the front door unlocked, you're spending money and time protecting the wrong assets.*

Recommendations for organizations by maturity level:

LOW-Level Maturity: Identify the gaps and fix them.

1. Get started with some risk modeling, and assess against foundational security controls.
2. Ask yourself: Where are the easy wins? Where are the big risks?
3. Get to work fixing them.

MID-Level Maturity: Enhance security maturity.

1. Devise a comprehensive road map that's integrated into all areas of the business.
2. Push toward higher maturity levels by mapping out process improvements and potentially investing in more advanced technology.

HIGH-Level Maturity: Continuous improvement.

1. Continuously improve your programs.
2. Ask yourself:
   - Where can we be more efficient?
   - How can we enhance cybersecurity awareness across the organization?

LESSON 2: Address the human element in the room.

Since 2020, 4 out of 5 of organizations have been hit with some kind of phishing attack. On top of that, according to Cybercrime Magazine, 4 companies were hit with malware every minute.

Looking Back: New Spins on Old Favorites

As the workforce moved to remote work environments in 2021 and 2022, threat actors have leveraged popular collaboration tools like Microsoft Teams and Microsoft OneDrive to join meetings, impersonate company leadership, and lure employees to open malicious files.

As of 2022, phishing attacks evolved beyond malicious email attachments and embedded links into more sophisticated, calculated social engineering attacks.

Callback Phishing

In a callback phishing scheme, a phishing email gets the target victim to call a "customer service" number for a subscription renewal or a bill. The attacker then has the trust of the target and can obtain highly sensitive information such as financial information, social security numbers, or login credentials.

Multi-Factor Authentication (MFA) Attacks

With MFA attacks (or MFA fatigue attacks), cybercriminals bombard their victims with repeated MFA notifications to trick users into authenticating. This tactic can be surprisingly successful, especially when the target victim is distracted or overwhelmed by the notifications or misinterprets them as legitimate authentication requests. The most famous example of this attack was conducted by Lapsus$ and targeted Uber in September 2022.

Hacktivism

While cybercrime can be quite lucrative, it does not mean that all hackers are in it for the money: some just want to send a message. A recent example of hacktivism in 2022 was the Russian-based threat actor, Killnet. It sparked quite a bit of chaos this past year using the classic DDoS attack to take down prominent organizations and public figures like the Elon Musk-owned company, Starlink, Whitehouse.gov, and the Prince of Wales, citing their outward support for Ukraine as the driver of the attack.

Related Content: *2022: Common Indicators of a Phishing Attempt*

Looking Ahead: End-User Training is More Crucial Than Ever

Just as ransomware as a service (RaaS) made it easier for unsophisticated attackers to deploy ransomware in recent years, in 2023, we can expect to see threat actors leveraging advancements in machine learning and AI to scale attacks, remove barriers to deployment, and equip hackers to scale social engineering, phishing, and malware attacks.

That said, it's easy to forget that in cyberwarfare, technology is a tool – and only part of the solution. At the end of the day, humans are on both ends of a breach. The human element was critical to more than 80% of breaches last year. And the best tool for mitigating that kind of risk? Training.

The good news? Regardless of your organization's level of cyber maturity, there are practical steps you can take to stay protected.

No longer should training be a one-time, annual event to check a box. Companies need to build robust training around attack methods and the tools they use to ensure adoption and compliance.

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Institute a training program and educate your workforce on a regular basis.
2. Leverage training that is actually interesting and engaging - not just parroting the "check-the-box" mindset.
3. Implement basic data protection processes and technology.

MID-Level Maturity:

1. Put your employees to the test with simulated phishing campaigns.
2. Invest in good tooling.
3. Gamify cybersecurity awareness training.
4. Build a comprehensive data protection program.

HIGH-Level Maturity:

1. Build a culture of cybersecurity awareness across the entire organization.
2. Integrate training, data protection, and insider risk with advanced threat monitoring and response.

LESSON 3: IoT & OT security threats.

As a rule, cybersecurity risk rises as our world becomes more interconnected. Business needs and competitive landscape pressures businesses to create or adopt new technology so fast that, in their desire to get to market first, they do not always address the inherent risk in doing so.

Looking Back: More Connection Meant More Risk

There was a time when only companies with a shop floor had to be concerned about IoT and OT risks. With the influx of Internet of Things (IoT) and 'all things connected,' this has created an entirely new arena for security concerns, bringing these kinds of issues to everyone's attention. Many of those 'air gapped' systems we assumed were safe we came to find out were actually connected because security was not a part of the operational technology (OT) side of the house. Today, we are seeing the convergence of OT & IT + IoT.

New technology to help assess and manage this IoT/OT risk is reaching a strong level of maturity. And yet, many industries heavy in IoT & OT are still not implementing it… and that has led to some major consequences.

Looking Ahead: Weaponized IoT/OT & the Edge

Hacking has been loosely linked to some casualties in recent years, but the current environment suggests that the weaponization of IoT and OT to drive catastrophic outcomes is on the rise. There are many critical systems within healthcare, manufacturing, critical infrastructure (ICS/SCADA), energy, utilities, the automotive industry, and more that could be (and often are) exploited in a wide-scale breach or attack.

As geopolitical tensions continue to rise, nation-states are increasingly turning to cyberwar instead of actual war to levy attacks on their political opponents. Therefore, we will likely see even more exploitation of IoT and OT devices in this context moving into 2023.

NEWS:

Ransomware attack at German hospital leads to death of patient

As IoT & OT extends the 'edge' and creates more attack vectors, companies need to conduct a threat assessment on new appliances they get for the office, in addition to extending their monitoring activity to any new potential attack vector added to their attack surface. This concern should also extend to partners and vendors who are using connected equipment as well.

In addition, advancements in edge computing and 5G will begin to challenge some of the traditional security in place, emphasizing physical security as well as new tooling to protect these devices at a deeper level. This will be prevalent in the manufacturing and automotive industries, in particular.

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Maintain an accurate inventory of assets.
2. Validate your assumptions around risk & security specific to IoT & OT.
3. Assess your risk against compliance requirements.
4. Continually train employees on a recurring basis.

MID-Level Maturity:

1. Conduct threat modeling.
2. Pentest your environments.
3. Implement security monitoring with patching and vulnerability management.

HIGH-Level Maturity:

1. Achieve integrated monitoring with SOC or MSSP.
2. Assemble a full-scale vulnerability management program that includes regular pentesting.
3. Push towards more advanced testing (like red team exercises).

Related Content: *The Top 5 Cyber Threats within the Manufacturing Industry*

LESSON 4: Cyber insurance rates & requirements are increasing.

The cost of a breach extends beyond the hard dollar cost of remediation. It incurs legal costs, operational costs, and perhaps most importantly: reputational costs. The concept of digital trust is more important now than ever before - especially as attacks on major organizations flood news headlines seemingly every day. ISACA defines digital trust as: *"the confidence in the relationship and transactions among providers and consumers within the digital ecosystem."*

Customers expect companies to protect their information. And whether that information is basic or highly sensitive, all it takes is one breach to obliterate any digital trust that they once had in your company. And that cost can radiate throughout all aspects of your business.

Looking Back: Rise of Cyber Insurance Premiums

While it's true that more and more companies are investing in cyber insurance coverage, according to a 2022 survey, only 19% of companies had cyber insurance coverage above $600,000, and 55% of companies did not have any insurance at all.

With the average cost of a data breach in the US coming in at over $9 million (IBM cost of breach report), it's safe to say that cyber insurance is no longer a "nice-to-have." But that doesn't mean obtaining cyber insurance is an easy feat.

Because here's the thing: over the past few years, cyber insurance providers have been hemorrhaging money because so many businesses are getting attacked. And make no mistake, these cyber insurance companies are adjusting their qualification criteria accordingly.

That means MORE...

- Rate increases
- Stringent requirements
- Critical scrutiny of applicants
- Denials of insurance claims

Cyber insurance has changed since the early days.

"In the early days (not really that long ago), some businesses thought cybersecurity insurance meant they didn't have to actually 'do' security. That has changed. The insurance companies know better and are working hard to manage their risk."

> Wil Klusovsky
Chief Security Architect at Avertium

Looking Ahead: Stop Checking the Box and Start Using Security Assessments (and possibly cyber insurance) to Reduce Risk

Many companies technically have cyber coverage, but once they're actually hit with a breach, they realize that their policy wasn't as comprehensive or helpful as they'd hoped. Whether they simply didn't purchase enough coverage or didn't meet certain requirements, there are many unfortunate situations where the payout just never comes.

If you're looking to fortify your cyber insurance coverage, make sure you understand the requirements and expectations of the policy. Some requirements that companies often misinterpret or fail to meet include:


Conducting an annual risk assessment


Maintaining a risk register


Active monitoring of their network


Engaging in regular penetration testing, and more

As threat actors expand their reach across industries with motivations that vary from one attack to the next, anyone could be the next big target. Cyber insurance is an effective measure in reducing the financial fallout from a breach, but it's becoming increasingly more difficult and expensive to come by.

If you already have cyber insurance, the next question becomes: Is it enough? Do you have the right type of coverage?

Whether or not you have or are exploring cyber insurance, as we move into 2023, every company must assess their environment in order to protect it – and do so thoughtfully, without a "check-the-box" mindset.

Some important questions to ask and get answers to include:

- Where is our sensitive data, how are we protecting it?
- Where are we most vulnerable, how likely is a breach?

Related Content: *Cyber Insurance: Is Advanced Protection Worth it?*

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Evaluate what kind of coverage you would need and weigh it against cost and risk.
2. Consult with your legal team.

MID-Level Maturity:

1. Confirm requirements for coverage and ensure you have a clear action plan to meet those requirements.
2. Align insurance with maturity planning.
3. Identify a partner that you can consult with in security planning and improvement.

HIGH-Level Maturity:

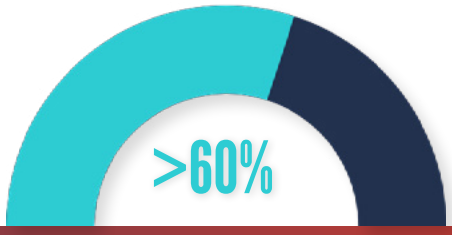
1. Extend requirements to supply chain / third party vendors and program management.

LESSON 5: Secure your supply chain.

While third party vendors can both lessen the burden on companies and expand their offerings to customers, entrusting sensitive information with a partner carries several daunting implications.

Looking Back: Supply chain breaches were caused by both partners and cloud-based or web-based applications.

More than 60% of breaches last year were related to the supply chain.



This is, in part, due to organizations failing to assess the risk of doing business with many of their partners. That said, remotely sharing data through the cloud or web-based applications also ties into third party risk.

Looking Ahead: Build a Robust 3rd Party Risk Management Program

As we move into 2023, the bottom line is this: The importance of assessing and managing the risk of every company you interact with and every technology cannot be overstated.

Any data sharing must be done securely, as every single interaction, every single shred of data shared between organizations is a potential entry point for attackers. Web apps have been and will continue to be one of the top attack vectors for breaches, and the increased societal need to connect and integrate exacerbates the potential for loss as companies communicate virtually with vendors.

By 2025, 60% of organizations will use cybersecurity risk as the primary determinant in conducting third-party transactions and business relationships. Because third-party risk is brought upon an organization due to their external ecosystem or supply chain, the companies who practice good cyber hygiene will have a distinct competitive advantage when trying to win business with security-aware companies.

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Identify high risk vendors and include obligations related to cybersecurity in any contract.
2. Assess your vendor's cybersecurity posture, and demand remediation before sharing information with any vendor who has poor cybersecurity hygiene.

MID-Level Maturity:

1. Establish a program to integrate into business processes.
2. Assign resources or services to track and manage third party risk management.
3. Create an efficient process to simplify vendor management.

Related Content: *You're Secure - But are Your Vendors? Assessing Third Party Risk*

HIGH-Level Maturity:

1. Assess key vendors.
2. Build a self-assessment program for lower risk vendors.
3. Staff or consume services for program management and auditing.

LESSON 6: Data privacy is only getting tougher.

Virtually every consumer has been a part of a data breach. And as consumer awareness grows around just how much money companies are making from selling their personal data, so will their demands for increased data privacy regulations and greater investments in the protection of their personal information.

Looking Back: Crack-Down on GDPR Violations

2022 was a time when GDPR violation fines reached record highs on big names like Meta and Google.

Alongside the growing enforcement of established privacy legislation, new legislation emerged as well, such as the American Data and Privacy Protection Act (ADPPA), passed by the US House of Representatives in June 2022.

The focus on data privacy did not just occur at the government level, however. A noticeable shift at the consumer level occurred as well, as people began to pay attention to how their data was being used, sold, and stored. According to Pew Research Center, 79% of Americans claimed they were concerned about how companies use their data, and over half of respondents to another survey believed it was more difficult in 2022 than ever before for companies to earn their trust [Salesforce].

Despite the fact that data privacy was solidified as a top concern for consumers and governments alike in 2022, many companies still seem to underestimate the cost of poor data management.

Looking Ahead: Get a Proactive and Actionable Data Privacy Plan in Place

Compliance is critical as regulations become more strict and fines become more costly. Several states have drafted comprehensive consumer privacy laws to take effect in 2023, many with broad, vague standards that leave companies liable and at-fault in many circumstances [Reuters]. Implementing a proactive and actionable data privacy plan - and taking action when needed - is critical for the internal and external success of any company managing extensive amounts of data or any sensitive data.

The collection and use of consumers' personal information will be further restricted as we move into 2023 and companies are well-advised to implement compliance measures proactively. By creating a rigorous data privacy program and keeping a legal team close by, companies can establish processes and procedures that get ahead of the thorough data privacy laws that will undoubtedly soon emerge across the nation.

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Identify which regulations you must comply with.
2. Build controls, policies, and procedures to properly maintain data protection and classification in order to meet data privacy requirements.
3. Engage legal counsel.

MID-Level Maturity:

1. Build or improve asset management systems.
2. Identify and evaluate which vendors you flow down/up to for other regulations.
3. Implement technology to assist in data protection, classification and governance.

HIGH-Level Maturity:

1. Proactively manage your assets and vendors around data privacy.
2. Establish a compliance program to monitor new and / or changing applicable regulations.
3. Have a Data Privacy Officer.

LESSON 7: Searching for security talent.

According to the 2022 (ISC)2 Cybersecurity Workforce Study, the cybersecurity workforce is facing a shortage of almost 4 million workers. The need for cybersecurity professionals is constantly climbing, but that also coincides with a need to pay higher wages, hire more experienced individuals, and rapidly train entry-level hires - none of which are necessarily easy asks.

Looking Back: The Broken Approach to Cyber Talent Acquisition

In the past, cyber talent acquisition has been inefficient and antiquated. Though tens of thousands of cybersecurity jobs were created in the past year, many of them require broad skill sets and extensive experience - leaving a massive amount of entry-level and specialized hires out of work.

It doesn't help that the job descriptions many companies advertise were and still are incredibly aspirational, spanning several requirements that are often not necessary to do the job. As a result, despite how qualified or capable a candidate may be, many have been dissuaded from applying to these roles due to the endless list of demanding qualifications listed on the job description.

Looking Ahead: Stop Looking for the Unicorn – Start Investing in Specialized Skill Sets

The lack of structure in many cybersecurity roles has created a demanding work environment in which employees are expected to wear several hats. By simplifying job descriptions and expecting only one role to be fulfilled by each employee, companies can both streamline operations and more successfully fill critical positions. Finding specialized talent rather than a team composed of jacks-of-all-trades can remove friction from training and onboarding and will likely attract more experienced talent as well.

Because many roles on the market require extensive experience, companies can start from the ground-up and invest in both training and tooling that makes more junior employees more effective, more knowledgeable, and equipped to improve their skill set and actually succeed in their role.

If gaps persist or if budget is limited, companies can also turn to managed security service providers and / or consultants for a more cost-effective and viable solution.

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Leverage third party partners, virtual CISOs, or security firms for projects.
2. When recruiting, let go of the mindset that a given degree or certification is required, instead opting for candidates that are ready and able to do the job.
3. Turn your focus away from experience and certifications and more towards capabilities of new hires.
4. Build a Diversity, Equity, and Inclusion (DEI) program or if one already exists, apply it to security and hiring practices.

MID-Level Maturity:

1. Prioritize focused skill sets rather than searching for a "unicorn" hire.
2. Simplify job descriptions to attract higher volumes of skilled talent, know must haves and hire for those.
3. Train the talent acquisition department and hiring managers to increase their understanding of what makes a quality security hire.
4. Create strong and flexible career paths and plan a trajectory for employee growth.
5. Apply DEI practices to job searching and seek out unique perspectives and backgrounds when hiring.

HIGH-Level Maturity:

1. Develop a fortified, repeatable onboarding / training program for new hires, especially those in entry-level positions to maximize their likelihood of success.
2. Understand promotions are no longer a flat percentage increase and scale appropriately for the pay of a new external hire.
3. Instill DEI practices in corporate ethos, looking to DEI principles to guide and inform all aspects in the business, starting with hiring and permeating throughout all internal processes and security initiatives.

LESSON 8: The Cloud is both your friend & your foe.

While it's true that the reliance on the cloud has created enormous efficiency, it has also created risk. The rapid migration to the cloud for companies across the world simply did not provide enough time for the technology to catch up, and many companies are unaware of the regulatory implications and risk they undertake when they adopt cloud-based solutions.

Looking Back: The Lack of Focus on Cloud Security Created Major Problems

The reality is, the cloud solutions are not always fortified enough to protect against more evasive or advanced threats, yet it's where more and more companies are entrusting their most valuable, sensitive assets. Much of the responsibility to adhere to regulations and protect information falls on the users of these solutions, and without experienced practitioners or a mindful leadership team, keeping up with the more technical aspects of remote sharing tools often falls to the wayside.

That said, cloud security has become critical in the past year. In 2022, the White House issued an Executive Order to advance the country's cybersecurity firms towards Zero Trust architecture, expanding requirements and placing an urgency on cybersecurity firms to adhere to best practices.

The Executive Order states that the Federal Reserve will comply with Zero Trust, and as a result, many major cloud providers and vendors are adjusting to meet the same requirements. Security leaders like IBM, Microsoft, ZScaler, and more have already implemented Zero Trust frameworks in response to the EO, and whether a company employs Zero Trust is an increasingly common subject explored in breach reports.

Looking Ahead: Zero Trust Will Likely Emerge as a National Standard

Zero Trust is more than just a buzzword, it's emerging as a national standard - not to mention that it's an effective defensive strategy when working in the cloud.

As we move into 2023, firms should evaluate whether implementing a Zero Trust framework should be a priority sooner rather than later, especially as more companies and governmental entities begin adding ZTN requirements to reduce third party risk. That said, whether that happens in the near or mid term, we're talking about making changes to your fundamental security strategy and that stuff doesn't happen overnight. If you see it on the horizon, starting now can ensure that your organization is future-ready.

Understanding your security posture within the cloud and what's required of you is critical to avoid both compliance errors and incoming attacks. Developing and adhering to a security framework like Zero Trust can remove some uncertainties regarding compliance and regulations moving into 2023.

Recommendations for organizations by maturity level:

LOW-Level Maturity:

1. Assess your current and future usage of the cloud and any associated requirements.
2. Review contracts with third party vendors to understand where responsibilities and liabilities lie.
3. Build a simple and actionable zero trust strategy.

MID-Level Maturity:

1. Implement processes and controls to protect data and monitor compliance.
2. Incorporate security requirements into new systems and integration processes.
3. Assess your identity stack and where it needs additional maturity.

HIGH-Level Maturity:

1. Implement modern identity and access controls.
2. Require a robust Zero Trust framework across all lines of business.
3. Collaborate with leading vendors to influence the long-term direction of Zero Trust for your organization.

CONCLUSION

PREPARE FOR THE 2023 THREAT LANDSCAPE

Where does your cyber maturity stand? Cybersecurity is an increasingly high priority for enterprises around the world, but a lack of standardization means that all organizations operate at varying levels of cyber maturity. Some invest the bare minimum in cybersecurity to simply check a box while for others,

Related Content: *6 Steps to Implementing a Zero Trust Network*

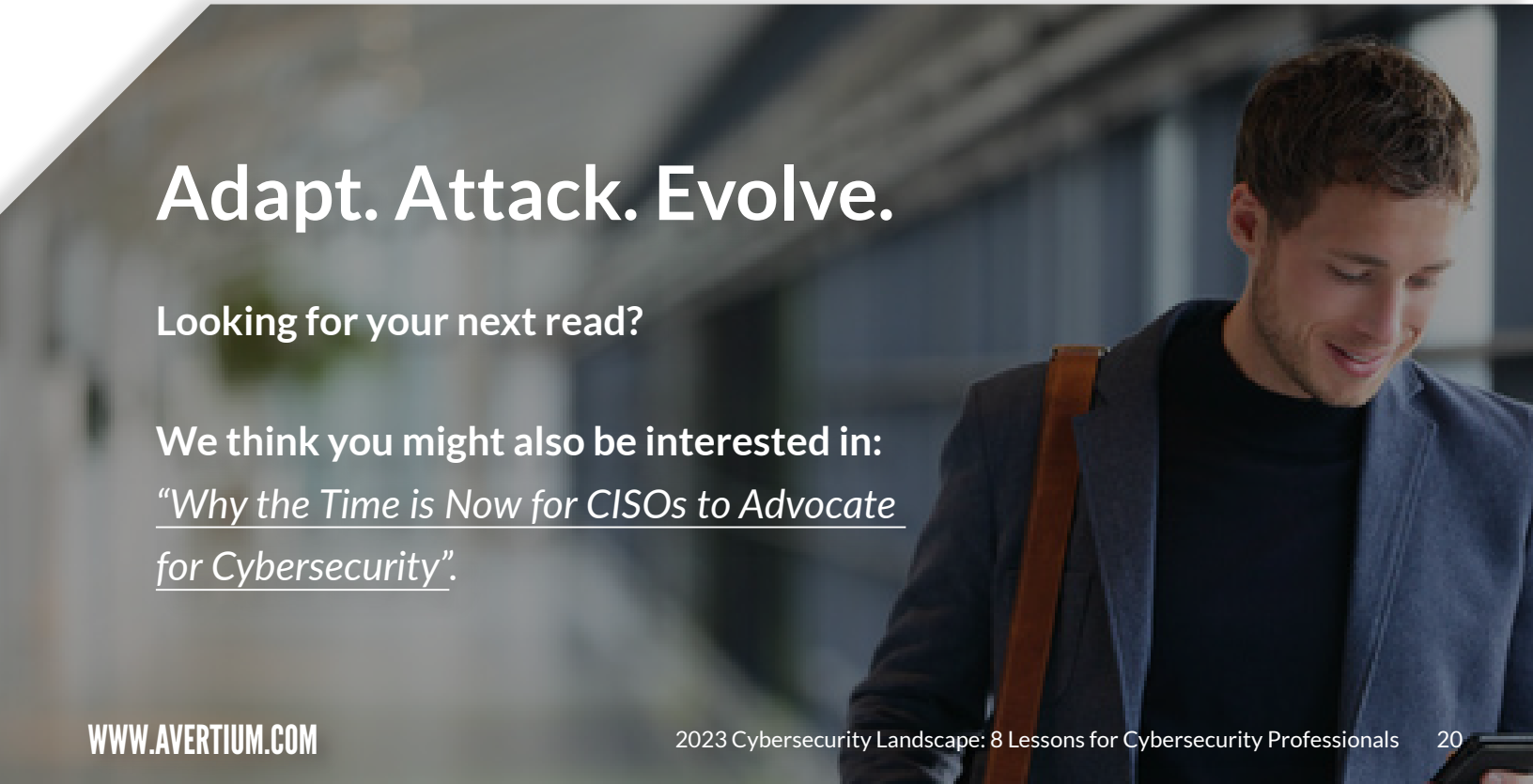
it's ingrained into their company's most integral activities. Knowing where their cybersecurity coverage stands is key for today's organizations as they navigate an ever-changing attack surface and strive to protect their most valuable assets.

HOW AVERTIUM CAN HELP

As we move into 2023, the need for big-picture, strategic thinking has never been greater. Many cybersecurity tools available today are mere point solutions that provide quick fixes for problems that will simply re-emerge as threat actors advance their approach.

At Avertium, we believe that the best security is a strategic, planned, and adaptable journey rather than a disparate collection of point solutions. We also believe that building cybersecurity resilience requires a calculated, methodical plan that builds cyber maturity in a way that can adapt, attack, and evolve alongside the ever-changing threat landscape.

Wherever the gaps are in your security strategy, Avertium is there to help you build cyber resilience through a comprehensive, programmatic cybersecurity strategy that connects to the business context, employs a cyber fusion philosophy, and leverages a human element to attack the chaos of today's cyber landscape with context. Show no weakness.



ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why **over 1,200** mid-market and enterprise-level organizations **across 15 industries** turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

CONNECT WITH US

AVERTIUM®

Cyber Fusion Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

SHOW NO WEAKNESS®