DEEP seas

The Deep Dive: Cyber Defense in 2024

A Special Report on Potential 2024 Cyber Threats

Contents

Threat actors are using artificial intelligence (AI), data theft, sophisticated ransomware, the dark web, and other technologies and techniques to create a more perilous cyber threat environment in 2024.

Leveraging research from TechTarget's Enterprise Strategy Group and real-world expertise from DeepSeas, this special report provides a deep dive into the cyber threat landscape for 2024, with a look back at key events and trends from 2023.

The focus of this report is on what's really happening across the threat landscape - eliminating hype and unnecessary fear tactics - to provide CISOs, CIOs, and their teams with expert guidance on how to mitigate risk in a rapidly changing world.

Each year brings innovations in threats from cyber criminals.

Following breakthroughs in 2023 that changed the threat environment, 2024 promises a new generation of threats leveraging AI, data theft, spear phishing, sophisticated ransomware, and more.

As threats become more sophisticated and dangerous, CISOs and CIOs are facing enormous pressure to mitigate risk and improve cyber resilience, while continuing investments in cybersecurity training, education, and awareness.

At the same time, organizations are dealing with an ongoing shortage of skilled cybersecurity personnel that shows no signs of abating in 2024. In addition, cyber leaders perceive a growing need to consolidate and centralize cybersecurity technology, management, and threat protection to take advantage of advances in automation, AI, and machine learning.

Research from TechTarget's Enterprise Strategy Group (ESG) and insights from the cyber defense experts at DeepSeas provide real-world guidance on some of the most critical challenges facing CISOs and CIOs in 2024, including dealing with AI-powered threats and ransomware and maximizing the value of real-time threat intelligence.

In 2023, more than one half of information technology (IT) professionals and business leaders said security operations were more difficult at their organizations than they were two years previously, according to an ESG Research Brief on the use of Generative AI in cybersecurity.[1] Among the top challenges they named were:

- **Constant firefighting -** More than one third of organizations (34%) said their cybersecurity team spends most of its time addressing emergencies and does not have enough time for developing strategy and process improvement. As noted by ESG, "This high-stress environment often leads to human error and staff burnout."

- **Monitoring security across a rapidly changing attack service -** One third (33%) of organizations found this task challenging as the attack surface constantly grows and changes, driven by factors such as digitization, third-party IT connections, and the growing use of the public cloud. More than three quarters of organizations (76%) said they experienced one or more cyber attacks resulting from an unknown, unmanaged, or poorly managed internet-facing asset within their attack surface.

- **Operationalizing threat intelligence -** Nearly a quarter of organizations (24%) said they are challenged with collecting, processing, analyzing, or acting upon a continuous stream of threat intelligence. Per ESG, "This challenge is aggravated because of a general lack of threat intelligence analysis skills."

These challenges manifest themselves in many ways.

These challenges manifest themselves in many ways. In a separate study from ESG, nearly two thirds of organizations (65%) said in the past year they were the victim of a successful ransomware attack that had a negative financial impact or disrupted business operations. Of these organizations, nearly one half said they suffered more than one successful ransomware attack. Typically, these organizations suffered large amounts of data being exposed to ransomware attacks - a mean of 1.3 petabytes - and only 16% said they were able to recover all their data. To get their data back, 56% of respondents said they paid a ransom.[2]

Given these challenges, what should CISOs, and CIOs be looking for across the threat intelligence landscape in 2024? More importantly, what can they do to mitigate the risk of successful breaches?

Working in concert, ESG Principal Analyst Dave Gruber and cybersecurity experts at DeepSeas have outlined five critical cyber threat challenges for 2024. An overview of each trend is provided, with an eye on what cyber leaders can expect in 2024. This report includes expert guidance, including steps cyber leaders and their teams can take to mitigate risk from each of these threats. This report also looks at the impact of additional issues across the cybersecurity landscape, including the role of the dark web and the growing danger of state-sponsored threats.

Threat Intelligence Deep Dive 2024: Five Trends That Will Change the Landscape

Trend 1: AI Evolves from Tool to Weapon

When ChatGPT was introduced in late November 2022, cyber criminals were among the first to jump on the technology, using AI to make attacks more potent and effective.

In 2023, ChatGPT and other AI bots were tools used in various nefarious ways:

- In business email compromise (BEC), phishing, and spear phishing to send more legitimate-sounding emails, tailoring messages with details to exploit vulnerabilities among specific employees
- To create more sophisticated malware, using AI analytics to analyze vulnerabilities and AI bots to automate, accelerate, and scale the number of attacks carried out
- To bypass security measures like CAPTCHA or biometric security checks with AI tools trained in pattern recognition

This is just the beginning, as criminals leveraged AI in 2023 as a tool to make existing attack techniques, tactics, and procedures (TTPs) more effective. What happens next should be of even greater concern to CISOs and CIOs: the use of AI as a weapon and a new entry point from which to launch attacks.

With the popularity of ChatGPT, individuals throughout organizations are using AI for all types of business purposes - to create more targeted marketing campaigns, to improve customer service, and, increasingly, to write software code. These uses of AI are typically unchecked and uncontrolled because they are out of view of the watchful eye of cybersecurity or IT teams.

This opens new vulnerabilities. In particular, DeepSeas recommends that cybersecurity and IT professionals pay close attention to these threats in 2024:

- **Malicious prompt injection -** Threat actors manipulate code within AI so it provides malicious or inaccurate prompts in software development. Criminals are exploiting ways to use AI to inject malware into code or change lines of code unbeknownst to the programmers writing that code.
- **Data poisoning -** Threat actors manipulate data within AI so it ignores certain data or provides malicious data, causing it, for instance, to ignore specific phishing emails or malicious transactions used in BEC scams.
- **SEO poisoning -** AI is used to manipulate search engine algorithms to prominently display malicious web sites that host malware, phishing schemes, or other harmful content.

- **LLM attacks -** These types of attacks access the large language model (LLM) used for AI. Since organizations need to provide a substantial quantity of sensitive information to get the most out of AI, this could lead to a backdoor attack within the AI software itself, giving threat actors access to that sensitive information. LLMs can also be susceptible to attacks where slight, carefully crafted changes to input text can lead to drastically different or erroneous outputs.

? Will all of these types of attacks happen eventually? **Yes.** Will they all happen in 2024? **Probably.**

ESG Perspective from Dave Gruber

Cybersecurity teams must focus on generative AI on three parallel trajectories:

1. Given the pace of experimentation, adoption, and overall enthusiasm for how and where generative AI can fuel new opportunities for growth, security leaders must appoint a team member to stay on top of internal projects to ensure they progress in a secure manner.
2. As adversaries leverage generative AI to advance attack TTPs, defensive technology must employ similar AI-based models to anticipate and detect a massive growth in attack variations. Security architects need to be actively engaged with solution and service providers to ensure the defensive tech-stack is adequately equipped to keep up.
3. Generative AI creates an opportunity for improvements in security operations activities, helping analysts more rapidly investigate and mitigate attacks. Security operations (SecOps) leaders need to actively experiment and invest in these tools to provide leverage for their teams.

By working with an advanced security partner such as DeepSeas, organizations can leverage synthesized intelligence to monitor threat actors and offensive tactics used in the real world. Partnering with an organization that has deep expertise is an invaluable benefit in keeping up with a landscape as dynamic and volatile as the one we expect in 2024.

Trend 1: AI Evolves from Tool to Weapon

DeepSeas Recommended Risk Mitigation Strategies

1. Limit the exposure of LLMs, which can include restricting public access. Implement output sanitation processes, in which the responses of LLMs are checked for potentially malicious content before being relayed to the user.
2. Use trusted data sets for AI training to limit risk of data poisoning. Periodically audit the data sets used for training AI systems, looking for inconsistencies or patterns that might suggest tampering.
3. Use advanced monitoring tools that leverage AI and machine learning to detect patterns of AI-driven attacks.

Trend 2: Operational Technology (OT) Attacks Cross a New Line

A significant focus for operational technology (OT) is in manufacturing environments, particularly with industrial control systems (ICS) and supervisory control and data acquisition (SCADA). As organizations evolve to Industry 4.0 models, they are converging IT and OT, with the converged IT/OT market expected to grow by 14.3% a year between now and 2030.[3]

IT/OT convergence offers manufacturing organizations benefits such as improved productivity and data utilization; cost savings through predictive maintenance; enhanced agility and resource management; improved regulatory compliance and quality control; and real-time decision-making.

However, IT/OT convergence also comes with increased security risks. “Cybersecurity teams must understand that there are certain risks that you just have to accept in an OT environment,” according to Jonathan Womack, a Senior Cyber Threat Intelligence Engineer at DeepSeas.

“If manufacturing is forced to turn off production, they will feel like they are burning money, so they aren’t likely to do it,” Womack adds. “If there is malware on a particular device in an OT environment, as long as that malware is contained to that box, cyber teams may have to be willing to accept that level of risk.”

“On the other hand, cyber teams have to convince OT teams of the overall business value of preventing attacks,” Womack says. “One way to do that in 2024 will be to develop methods to measure and monitor return on investment (ROI) for cybersecurity.”

According to DeepSeas, these are among the most critical cyber threat challenges in IT/OT convergence to address in 2024:

- **An increased attack surface -** This is exacerbated by the growth of IoT devices, which pose particular vulnerabilities as well as the growth in edge computing.
- **Legacy systems vulnerabilities -** Many OT systems were designed and implemented before cybersecurity was a consideration. Integrating these legacy systems with modern IT networks can expose them to threats they were never designed to face.
- **Lack of visibility, monitoring, and consistent standards -** OT environments often lack the sophisticated monitoring and visibility tools found in IT networks. This can make it difficult to detect and react to cyber threats promptly. OT systems often come from different vendors and eras, leading to a mix of protocols and standards.
- **A cultural chasm -** IT and OT leaders have different focuses. IT security often prioritizes data confidentiality and integrity, while OT security emphasizes availability and safety. In the manufacturing environment, any disruption in availability can cost millions of dollars. These environments cannot shut down to patch, nor can they stop production due to a security event.

ESG Perspective from Dave Gruber

The threat environment for converged IT/OT systems promises to be more perilous in 2024 as criminals seek to use OT as an entry point - not just against the OT systems, which can be crippling enough, but also for stealth attacks against IT systems, exploiting the interconnected nature of converged systems and networks.

As adversaries target vulnerable OT environments to either disrupt operations to motivate ransom payments or cross over into IT environments to gain access to valuable data assets, SecOps and OT teams must establish collaborative operating models that enable rapid response.

Incident response readiness planning and rehearsal must include OT leaders, and mitigation response actions must be customized to support OT operating requirements. Working with a partner like DeepSeas, who has experience with integrated security strategies for IT and OT infrastructure, can jumpstart the critical collaboration between cybersecurity, IT, and OT teams.

Trend 2: Operational Technology (OT) Attacks Cross a New Line

DeepSeas Recommended Risk Mitigation Strategies

1. **Close the cultural divide.** One of the most important steps organizations can take in 2024 is to close the cultural divide between IT/cybersecurity teams and OT teams. Cybersecurity teams must accept the reality that there will be some manufacturing equipment that will have malware on it. OT teams must accept the reality that convergence is a necessity and work with cybersecurity teams on finding points of compromise. OT teams also need to educate security teams on mitigation strategies that differ from typical IT security risk mitigation techniques.

2. **Develop a new ROI model.** OT teams have a fairly clear viewpoint on ROI: If we turn off production, we may lose money every minute. But how can cybersecurity teams reframe the investment so it is based on the business value of avoiding a breach? Are there areas of compromise in terms of patching and updates when production systems need to go down for other types of maintenance?

3. **Leverage joint threat detection in the security operations center (SOC).** Running threat detection for both OT and IT environments through the same SOC is a way to reduce risk. There are enough similarities across the environments that the same technologies, tools, and tactics can be used, giving SOC teams greater visibility across the entire organization.

Trend 3: The Ransomware Madness Continues

Enterprise Strategy Group (ESG) research reveals that 75% of organizations experienced an attempted ransomware attack during 2022-2023, with 11% experiencing attacks daily and another 16% weekly. Of these, 56% paid a ransom to regain access to data, applications, or systems, and 57% not only received additional extortion attempts, but also paid the extortion.[4]

Clearly, for cyber criminals, ransomware is working well. So why stop? Why not expand? And that is precisely what we expect cyber criminals to do in 2024 - expand their ransomware attacks and continue to go after vulnerable targets such as municipalities, public education institutions, smaller colleges and universities, and smaller healthcare organizations.

Perhaps 2023's biggest ransomware story was the MOVEit cyber attack, which affected more than 2,000 organizations with data thefts affecting more than 60 million people. The attack exploited a vulnerability in the widely used MOVEit managed file transfer software from Progress Software.

"One reason MOVEit was particularly frightening was because of its breadth, scale, and randomness," according to Aaron Bierlein, a Cyber Threat Intelligence Manager at DeepSeas. "There was also the scary reality that affected organizations had little control, actually none, in terms of prevention or remediation other than to pay the ransom."

Will 2024 bring attacks similar to MOVEit? Most likely, Bierlein says, noting that we can also expect these attacks to continue to evolve and evade defensive strategies. "Look for new types of extortion that will further motivate payments," Bierlein says.

Another important trend in ransomware is attackers obtaining multifactor authentication (MFA) credentials, according to Bierlein. Since most organizations use MFA as part of their security posture, this was an inevitable attack surface. However, previous methods, such as adversary-in-the-middle (AitM) attacks, are being replaced by simple attacks. For example, someone contacts a service desk posing as an employee and gets credentials sent to a personal email address controlled by the threat actor.

Two other important ransomware-related trends to watch out for in 2024:

1. **Demands and payments continue to rise.** In 2024, expect a continued rise in the amount demanded by attackers and a consequent rise in the amount paid to get data or operations back. According to one report, the average ransomware paid in 2023 was $1.54 million, nearly double the 2022 amount of about $812,000.[5] Attackers tend to stick with what's working.

2. **Lack of insurance is a reality.** When we look back a few years from now, we may look at 2024 as the year that the concept of cybersecurity insurance was declared terminally ill. According to ESG research, only 17% of organizations currently have cyber insurance policies. In addition, more than 60% question whether they can afford the rates and whether a policy can meet their future needs.[6] Instead of paying huge premiums for limited insurance coverage, more and more companies may just put that money aside to pay the ransom in case of a successful attack.

ESG Perspective from Dave Gruber

Ransomware preparedness is more important than ever, requiring broad participation from IT, cybersecurity, OT, and line-of-business leaders. While cyber insurance options are still available, depending on it to recover is not a sustainable strategy.

Effective backup and data recovery strategies are part of the solution, but much more is required to build resilience to ransomware. Security leaders, along with C-level support, must assign, fund, and monitor a continuous ransomware-preparedness program, with a defined leader and formally assigned members through all functions.

Managed Detection & Response (MDR) solutions, such as those offered by DeepSeas, can be an essential element in mitigating the risk of cyber attacks and are particularly valuable for organizations, such as municipalities or smaller institutions of higher education, that have limited cybersecurity budgets and in-house skills. Organizations can use DeepSeas for a variety of services aimed at identifying security risks and reducing attack surfaces digitally, physically, and socially.

Trend 3: The Ransomware Madness Continues

DeepSeas Recommended Risk Mitigation Strategies

1. Leaders at organizations that lack resources and don't have an endpoint detection and response (EDR) solution in place, should get started in 2024 with either a MDR solution or EDR as a service.

2. Ensure employees at help desks understand the new threat of MFA credential attacks. Provide regular awareness training on new types of threats throughout the entire organization. Also ensure that employees are aware of new vulnerabilities through voice-based and text-based attacks.

Trend 4: No Surprises Here – Humans Are Still Vulnerable

In 2022, BEC attacks led to $2.7 billion in losses according to the FBI.[7] The scale, scope, and volume of attacks increased in 2023 and will increase again in 2024.

Despite the best efforts of organizations to train and educate employees, and despite preventive tactics such as MFA, zero trust, and email authentication protocols, scams that entice humans to take actions and inadvertently bring harm to their organizations remain the number one source of successful cyber attacks.

The challenge for 2024 is similar to the challenges across the cybersecurity spectrum: BEC scammers are using tried-and-true methods - such as CEO fraud, false invoice schemes, and credential theft - while enhancing them with modern tools such as AI, machine learning, automation, and sophisticated social engineering.

For example, scammers are using AI to craft more legitimate-sounding emails from foreign language sources and adopting fully automated exploitation. Vishing (voice phishing), we predict, will become a more popular attack vector in 2024, as will using text via smishing (SMS phishing) attacks.

"Phishing-as-a-service kits available on the dark web allow access to less sophisticated threat actors, increasing the landscape of these attacks," according to Womack at DeepSeas. "We are also seeing a growing threat whereby threat actors target cloud instances with AitM attacks to gain credentials to cloud environments."

"AI is giving threat actors another tool to improve their social media tactics and conduct research, so they are more accurate in their BEC, phishing, and spear-phishing scripts," Womack adds. "Adversaries are using more believable language and honing scripts to appeal to the motivations and emotions of individual targets."

Threat actors are also using AI to be more adept at targeting vulnerable employees, such as those who are working remotely or in hybrid environments or have job functions in areas such as finance or human resources.

"Adversaries will browse social media and forums to search for specific employees and then gather information to personally exploit them to gain their credentials or download a malicious program," Bierlein says. "As people use more communication and collaboration channels, both sanctioned and unsanctioned, attacks will leverage more multichannel phishing techniques to evade security controls. Be on the lookout for this recent trend: scammers pretending to be job hunters and submitting resumes that contain malicious payloads."

ESG Perspective from Dave Gruber

As adversaries continue to leverage people to evade automated controls, cybersecurity and IT leaders must accept that humans are fallible and will fall victim to phishing and other impersonation tactics. Partnering with MDR providers such as DeepSeas can help operationalize the many aspects of securing human-oriented attack strategies.

Security architects must uplevel defense strategies to embrace a culture of distributed communications and collaboration and look for solutions that are architected to scale across multiple mechanisms. Monitoring and securing identity infrastructure will be a paramount tactic within 2024 strategies and should be prioritized among top investments.

Trend 4: No Surprises Here – Humans Are Still Vulnerable

DeepSeas Recommended Risk Mitigation Strategies

1. Continuous training and awareness programs are more important than ever in 2024. These should be mandatory for all employees, and organizations should strive to create a culture of cybersecurity awareness.

2. Training should be targeted for vulnerable employees, which could extend to specific departments such as human resources and finance, as well as to employees working from home, remotely, or in hybrid work environments.

3. Deploying zero trust frameworks and/or closely managing the principle of least privilege can mitigate risk and protect humans from causing breaches through ignorance, negligence, or malice.

Trend 5: Identity Re-emerges as a Highly Targeted Attack Surface

The human element is a major aspect of identity, with scammers using phishing, BEC, social engineering, and spoofing to trick individuals into revealing personal or login information.

These types of attacks also seek to take advantage of gaps in how organizations manage identities, and closing these gaps is one of the important initiatives for IT and cybersecurity teams to undertake in 2024.

"For years - decades actually - organizations treated identities like assets. Identity was tied to a specific computer, security code, serial number, and name," Womack says. "Identity was typically managed by the networking team within IT. If a device was stolen and the identity potentially compromised, you simply denied access to the network."

"One of the potential gaps in identity management is identifying who is in control," adds Womack. "As cybersecurity teams seek to gain greater control of identity monitoring and management, many are experiencing a cultural chasm, similar to the one between IT and OT teams."

Closing the cultural chasm is important in 2024 because IT and cybersecurity teams are expanding identity management functions to include persistent monitoring of identity usage. AI and machine learning are being used for behavioral analysis to detect anomalies in employee behavior that might indicate that their identity has been compromised. Zero trust strategies are also helping to manage, monitor, and control the principle of least privilege access.

ESG Perspective from Dave Gruber

If the process of migrating from identity management to identity monitoring hasn't begun in your organization, 2024 is the time to start. It begins with a comprehensive inventory of all identity infrastructure and a detailed audit of policies and operations.

Beyond specific identity monitoring and management, identity plays a key role in detection, investigation, and response activities, so architects need to ensure SecOps tools are identity aware. When it comes to managing identity, security service providers such as DeepSeas can help identify, implement, and operationalize controls and processes.

Trend 5: Identity Re-emerges as a Highly Targeted Attack Surface

DeepSeas Recommended Risk Mitigation Strategies

1. Addressing the cultural issue between networking and cybersecurity teams requires a clear articulation of who is responsible for managing identities and their underlying factors, including setting policies, enforcing policies, monitoring, and measuring outcomes.

2. Focus on where, when, and how extensively to deploy zero trust.

Threat Intelligence Deep Dive 2024: More Factors to Consider

In addition to the five major trends discussed above, CISOs and CIOs have additional important factors to consider in their 2024 cybersecurity strategies and investments. In this final section of the report, business and technology leaders at DeepSeas and Enterprise Strategy Group (ESG) share their perspective and final recommended actions.

Cybersecurity Personnel Shortage

The good news is that the cybersecurity workforce is at a record high. According to the 2023 ISC2 Cybersecurity Workforce Study, the size of the global cybersecurity workforce is 5.5 million, a 9% increase from 2022. The bad news is that the workforce gap is growing even faster. Between 2022 and 2023, the shortage increased by 13%, meaning that there are about 4 million cybersecurity professionals needed worldwide.[8]

One of the challenges in 2024 is a gap between the skills needed by organizations and those brought in by young professionals, many of whom have been attracted to the field because of the promise of finding a job easily. Cybersecurity is such a relatively new field that many individuals with new certifications are not receiving the education required to competently fill the jobs that are available.

Security teams are turning to Managed Detection & Response providers (MDRs) for help. DeepSeas is an advanced MDR helping companies of all sizes transform their cyber defense programs, including assessments, program strategies, implementation, security operations management, and incident response.

The Dark Web 2024

The dark web has been around for nearly 20 years and in a steady state of operation for close to five years, with numerous long-running actors facilitating cyber crime at a high level. This includes access brokers selling compromised credentials and services, ransomware groups, and exploit brokers that offer the latest and greatest software compromises. In short, the dark web has continued to provide fertile offerings to cyber criminals of all calibers. The dark web landscape is unlikely to drastically change in 2024; what exists fills the demand quite effectively.

Threat actors will continue to use online, semi-public forums and apps, such as Telegram, supplemented by user-to-user private messaging services, such as Tox or Element, to buy and sell goods and services related to cyber crime, much as they have for more than 20 years.

Recent leaks and compromises of some of these communication platforms may provide some opening for law enforcement. Still, without coordinated law enforcement activity worldwide, permanently ending a criminal group's operations is exceedingly difficult. Expect to see potential successes quickly turn sour as presumably disabled commodity malware groups resume operations in short order.

The Impact of State-Sponsored Threats

The landscape for state-sponsored cybersecurity threats in 2024 is probably the most perilous the world has ever seen. These types of threats are potentially more damaging and better funded than ever, taking advantage of emerging technologies and automation. What makes the situation in 2024 so concerning is the state of the world: the war between Israel and terrorist organizations, the war between Ukraine and Russia, as well as the increasing tensions between China and Taiwan, and the continuous threat from Iran and North Korea.

Organizations should be prepared for major disruptions if they are operating in any of these parts of the world. As we have seen in the past with state-sponsored cyber attacks, the potential downstream effect can upend businesses in many ways - disrupting supply chains, closing off potential markets, and causing rapid and major shifts in business strategies and budgets. Among the trends we are seeing are the use of deepfakes in warfare and the growing use of cyber proxies - e.g., Israel providing Pegasus spyware for Saudi Arabia to monitor dissidents.

A Pendulum Swing from the Cloud?

Yes, cloud computing has been revolutionary. But many of the reasons that organizations shifted to the cloud in the first place are no longer quite as relevant today as they were several years ago. First, cloud services have become extremely expensive. Second, they don't give organizations all the controls they need when it comes to cybersecurity.

Misconfigured cloud settings are a growing security threat leading to a range of security vulnerabilities and risks, including unauthorized access, data breaches, and service disruptions. It may just be a small trickle now, but do not be surprised to see more instances of small and medium businesses moving back to on-premises computing in 2024 to address concerns about cloud security and cloud costs.

Data Management

One of the other challenges with the cloud is that it represents another potential silo - or many additional silos - where data can either get trapped or lost. Data management is one of the biggest challenges in cybersecurity, with organizations trying not only to define what they consider to be their crown jewels but also identify just where those crown jewels are located.

Organizations are still seeing large numbers of applications being used across their operation with no technical oversight and, more importantly, no cybersecurity oversight. In 2024, we expect that organizations may increase their focus on data loss prevention and leverage AI as a growing tool for data classification and categorization.

Conclusion

It would be a significant understatement to say that 2024's threat landscape will be complicated. CISOs and CIOs are dealing with a world that is changing rapidly and where AI is creating vast new opportunities for those who would perpetuate cyber attacks and for those who would seek to prevent those attacks from succeeding. It's a world where the potential costs of breaches are measured in billions of dollars, and the impact of threats to vital infrastructure can include unthinkable consequences.

As noted throughout this combined Enterprise Strategy Group and DeepSeas special report, top considerations for making your organizations safer in 2024 include these actions:

- Leverage AI to anticipate and detect a massive growth in attack variations and help recognize the increased threat of AI-based attacks. This includes using advanced monitoring tools that employ machine learning to detect patterns of AI-driven attacks.
- Close the cultural divide between IT, cybersecurity, and OT teams to empower the business benefits of IT/OT convergence without creating additional risks of attacks, like ones that leverage OT vulnerabilities to exploit IT-based systems such as human resources, finance, or sales.
- Strengthen training throughout the organization and ensure that it is focused on areas such as BEC and phishing, where human errors and vulnerabilities can be both stealth and devastating. Make sure employees understand how to avoid falling victim to new ransomware threat vectors such as vishing, smishing, and MFA credential attacks.
- Explore technologies and frameworks such as zero trust, real-time threat intelligence, cybersecurity consolidation, SASE, and others that enable the organization to extend visibility and awareness, so SOC teams can be more proactive in eliminating threats and more responsive in mitigating potential damages.
- Complete a comprehensive inventory of all identity infrastructure and a detailed audit of policies and operations, so you can close gaps and make the necessary investments in people, technologies, and processes to prepare you for a more sophisticated cyber threat landscape in 2024 and beyond.

We hope this deep dive into the 2024 cyber threat landscape provides an overview of the key threats facing organizations and a better understanding of how these threats are affecting business and technology decision-makers. The year 2024 promises to be a breakthrough one for cybersecurity in many ways. Let's hope that most of the breakthroughs yield positive results and lead to peace and calm in the cyber seas.

Transform Your Cyber Program.

www.deepseas.com

References

[1] Source: Enterprise Strategy Group Research Brief, Cybersecurity Professionals Anticipate Many GenAI Use Cases, September 2023.

[2] Source: Enterprise Strategy Group Complete Survey Results, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation,November 2023.

[3] Source: "IT/OT Convergence Market Size (2023-2030)," Virtue Market Research, 2023.

[4] Source: Enterprise Strategy Group Complete Survey Results, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation, November 2023.

[5] Source: Sophos, "The State of Ransomware 2023," May 2023.

[6] Source: Enterprise Strategy Group Complete Survey Results, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation, November 2023.

[7] Source: Federal Bureau of Information, Internet Crime Complaint Center, "Internet Crime Report 2022."

[8] Source: ISC2 Cybersecurity Workforce Study, "How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce," 2023.

Acknowledgements

The 2024 Cyber Threat Outlook contributors:

Dave Gruber, Principal Analyst, Enterprise Strategy Group

Wade Alt, Chief Operating Officer, DeepSeas

Aaron Bierlein, Cyber Threat Intelligence Manager, DeepSeas

David Lavinder, Chief of Cyber Operations, DeepSeas

Jonathan Womack, Senior Cyber Threat Intelligence Engineer

DEEP seas