Devolutions

THE TOP 5 CYBERSECURITY RISKS FOR IT PROS IN 2025

JANUARY 15, 2025

OVERVIEW

Throughout 2025, we will see remarkable advancements and innovations across the digital world that will reinvent and redefine what is possible. However, there is a darker aspect to the story as well. In the months ahead, we will also see new cybersecurity threats emerge, while existing threats grow more dangerous and costly.

In this white paper, we dive into five critical cybersecurity risks for IT pros in 2025. In addition to exploring causes and consequences, we also share practical strategies and advice for IT pros to be proactive, get prepared, and guide their organization forward safely and successfully.

RISK #1

THE RISE OF ADVERSARIAL AI

According to the *CompTIA IT Industry Outlook 2024* report, 33 percent of organizations are using AI in a limited or moderate way, and 22 percent of organizations are aggressively pursuing AI integration across a wide range of operational workflows — including those that drive and strengthen cybersecurity itself.

Indeed, many organizations are already using (or will soon be implementing) AI to enhance threat detection, improve incident response, perform advanced malware detection, and thwart unauthorized login attempts by analyzing biometric data and user behavior patterns. That is the good news.

The bad news is that cybercriminals are also highly interested in AI; not to protect themselves, but to carry out attacks. This nefarious approach of using AI to manipulate AI systems by exploiting vulnerabilities or by introducing malicious inputs to evade detection is known as adversarial AI — and it has the potential to wreak havoc and cause plenty of sleepless nights for IT pros in 2025 and beyond.

Some types and examples of threats that involve adversarial AI include:

- Privacy breaches that steal data and commit identity theft. While this type of threat is not new, AI is enabling cybercriminals to carry out attacks with unprecedented speed, precision, and scale. For example, in late 2022, cybercriminals attacked T-Mobile by using an AI-equipped API to access the private data of around 37 million customer records that included their full names, contact numbers, and PINs

- AI botnets that carry out distributed denial-of-service (DDoS) attacks, perform credential stuffing, and perform large-scale attacks against targeted systems. For example, a few years ago, cybercriminals attacked Pulse Secure VPN by using AI algorithms to scan the internet for vulnerable servers, automatically compromise them, and add them to a botnet that was used to launch DDoS attacks against various high-value targets.

- Manipulating AI models (a.k.a. data poisoning) so they ultimately produce flawed outputs or make incorrect decisions. While this is not a conventional attack type designed to steal data and commit identity theft, it can be enormously destabilizing and costly for victims who have no idea that they have been targeted.

- Stealing the models used in AI systems, which for many organizations represents valuable and confidential intellectual property.

HOW IT PROS CAN FIGHT BACK AGAINST ADVERSARIAL AI

There are no easy answers or quick fixes for dealing with adversarial AI **(or, for that matter, any of the risks explored in this white paper).** Yet at the same time, doing nothing and "hoping not to get hit" is absolutely not an option.

The potential costs of a **cyberattack** are greater than ever before; not only for large enterprises but also for small and mid-sized businesses (SMBs). SMBs are increasingly under attack by **cybercriminals**, who are attracted by relatively weaker **cybersecurity defenses** (and, in some cases, essentially non-existent ones). According to a study by Accenture, 43 percent of all cyberattacks worldwide now specifically target SMBs. The *Devolutions State of IT Security in SMBs in 2023/24 Survey* revealed that 78 percent of SMBs are more concerned about cybersecurity than they were a year ago, and 69 percent **have** experienced at least one cyberattack in the last year.

Later in this white paper, we **will take a closer look** at how IT pros can protect their organization from the massive — and, in some cases, catastrophic — costs of a breach. For now, let us continue discussing how IT pros can fight back against adversarial AI. Global advisory firm Grant Thornton recommends an approach and plan that covers eight core areas:

- **Policies and Procedures:** Review and, as necessary, update existing policies and procedures to define AI-specific security requirements, designate roles to oversee AI operations, and ensure the implementation of security guidelines.

- **Threat Modeling:** Conduct threat modeling exercises to identify and assess the impact of potential security threats facing AI tools and systems (including the threats described earlier, such as privacy breaches and AI botnets).

- **Data Governance:** Ensure that data is properly classified, protected, and managed throughout its lifecycle. Governance aspects include identifying roles and responsibilities, data quality assessments, data validation, and acceptable data use.

- **Access Control:** Establish identity and access management (IAM) policies that address core questions such as: Who should have access to which AI systems and data? How and when should this access be re-evaluated? **What kind of** reporting, logging, and alerts must be in place? **What enhanced** access controls do we need if AI has access to personally identifiable information (PII) or other sensitive data?

- **Encryption and Steganography:** Use techniques such as watermarking (adding a digital signature) or radioactive data (minor modifications to a file or training data) to track AI models and ensure integrity.

- **Endpoint Security: Cybercriminals** have always favored targeting endpoints, such as laptops and mobile devices. What is new — and much worse — is **that** they are now using AI to scale up their attacks on endpoints, while making breaches even harder to detect. Endpoint security solutions augmented with user entity and behavior analytics (UEBA) can help spot early signs of an AI attack, so **the attacks** can be shut down before they go into high gear.

- **Vulnerability Management:** This includes robust security protocols, testing and validation procedures, and ongoing monitoring and maintenance. It is also critical for IT pros to regularly apply software updates and patches, as well as conduct regular assessments of AI infrastructure components to identify and remediate vulnerabilities.
- **Security Awareness:** Last but certainly not least, everyone in the organization must be aware of all cybersecurity risks (including but not limited to those related to AI) and trained accordingly.

RISK #2

THE RISE OF DEEPFAKE PHISHING ATTACKS

The practice of sending fraudulent emails and other messages claiming to be from reputable companies and trusted individuals — better known as phishing — remains a major threat. According to *IBM's 2023 X-Force Threat Intelligence Index*, phishing remains the leading infection vector, playing a role in 41 percent of attacks. **Additionally**, Verizon's *2024 Data Breach Investigations Report (DBIR)* found that the overall reporting rate of phishing has grown over the past few years, and the median time for users to fall for phishing emails is less than one minute.

These days, cybercriminals have added a powerful new weapon to their phishing arsenal: deepfakes, which involve using advanced technology to make phishing attacks tougher to detect — and therefore harder to prevent. Examples include:

Creating false profiles to lure victims. An analysis in 2022 by researchers at **the** Stanford Internet Observatory identified over 1,000 fake LinkedIn profiles that appeared to be AI-generated.

Using face-swapping technology to impersonate someone during video calls — which is precisely what a cybercriminal did in 2023 to get a victim to transfer $622,000.

Cloning someone's voice and leaving voicemails for a victim, or **even** engaging them in live, real-time conversations. An estimated 37 percent of organizations have already been hit by a deepfake voice fraud attempt.

WHAT IT PROS CAN DO TO DETECT AND THWART DEEPFAKE PHISHING

IT pros who want to keep everyone in their organization from falling victim to deepfake phishing attacks — and opening the gates for cybercriminals — should carry out the following:

- **Implement Multi-Factor Authentication (MFA):** Ideally, this should combine biometric data with other forms of verification such as passwords, PINs, or verbal confirmations through secure channels.

- **Train End Users:** Train end users to spot signs of potential deepfake phishing, and educate them on how **to** immediately and effectively report their concerns — even if it means pausing workflows or missing deadlines. **With regard** to video, end users should be on the lookout for things like out-of-sync lip movements, unnatural-looking facial hair, too much or not enough eye blinking, and strange shadows or light reflections **(or a lack thereof). Currently**, many deepfakes struggle with properly representing the natural physics of a scene. **With regard** to audio, end users should be alert for inconsistent background noise or ambiance, unnatural pauses or intonation changes, and robotic or stiff speech patterns. Of course, all of these clues **are not definitive evidence.** However, end users should be trained to err on the side of caution.

- **Implement the Principle of Least Privilege (POLP):** In this model, end users are given only the amount of access required to carry out their day-to-day job — and nothing more.

- **Use a Privileged Access Management (PAM) Solution:** This limits and governs end user access to systems, accounts, processes, and users. We discuss the importance of PAM later in this white paper.

- **Deploy AI-Powered Deepfake Detection Systems:** Use systems that employ techniques like photo plethysmography to detect real-time changes in blood volume in videos and audio forensics tools to analyze the spectrogram of voice recordings to identify synthetic tampering.

We are only at the beginning of the deepfake phishing era, and the full extent of what cybercriminals will attempt remains to be seen. However, IT pros who lead the way in equipping and preparing their organizations and end users will be in much better shape in the months and years to come **compared to** those that take a passive, wait-and-see approach — one that could cost their organizations dearly.

RISK #3

PRESSURE TO COMPLY WITH NEW CYBERSECURITY REGULATIONS

In 2024, several new cybersecurity regulations came into force around the world, and many IT pros (especially those in Europe) found themselves racing to meet compliance requirements before various deadlines. Some of the major regulations that have been introduced include:

- **The Network and Information Systems Directive (NIS2):** This directive entered into force on January 16, 2023, and member states had to adopt it into their respective national laws by October 17, 2024. The NIS2, an update to the 2016 NIS Directive, standardizes cybersecurity practices across EU member states and aims to foster stronger defenses, streamlined incident response, and improved cooperation within the EU.

- **The EU Cyber Resilience Act (CRA):** Adopted by the Council of the EU on October 10, 2024, the CRA mandates stronger cybersecurity measures across a wide variety of hardware and software products.

- **The Digital Operational Resilience Act (DORA):** This act establishes a regulatory framework for digital operational resilience, requiring financial entities in the EU to ensure that they can withstand, respond to, and recover from all types of information and communication technology (ICT)-related disruptions and threats. DORA comes into full effect in January 2025.

- **In the U.S.:** New SEC disclosure rules came into force in 2024, mandating organizations of all sizes to report cybersecurity incidents and disclose policies for risk management, security strategy, and governance.

- **ISO 27001 Transition:** Organizations currently certified to the ISO 27001:2013 standard have until October 31, 2025, to transition to the ISO/IEC 27001:2022 standard (or else their certification will expire or be withdrawn). While there is significant overlap between the two standards, there are notable changes around planning, defining process criteria, and monitoring.

Please note that the above is not intended to be a comprehensive list of all new cybersecurity rules and regulations introduced in 2024 or coming into effect in 2025 and beyond. However, it highlights some of the biggest changes and emphasizes that IT pros are not just under pressure from cybercriminals to bolster their organization's cybersecurity defenses — they are also under scrutiny from lawmakers and regulators, who are not reluctant to impose fines and sanctions for non-compliance.

WHAT IT PROS CAN DO TO COMPLY WITH NEW CYBERSECURITY REGULATIONS

CompTIA advises organizations to establish a **Cybersecurity Compliance Program** by covering the following core activities:

- **Create the Compliance Team:** This team should include individuals outside IT to ensure that cybersecurity is part of the organization's culture, and not just the responsibility of IT pros.

- **Set Up a Risk Analysis Process:** This process should cover identifying risks, evaluating risk levels, analyzing risk, and setting risk tolerances.

- **Establish Security Controls:** These controls should mitigate or transfer cybersecurity risks.

- **Document Policies:** Ensure there are clear guidelines that IT teams, end users, and other stakeholders must follow.

- **Monitor the Program:** Continuously monitor the program as new regulations emerge or existing rules are updated.

In addition, one of the most important and impactful things that IT pros can do to support their organization's compliance requirements is **focus on centralizing, protecting, and monitoring critical access points**. This involves implementing solutions that enable:

- **Secure Remote Access Management:** This should be augmented with session recording to capture and govern what end users do while a remote connection is open.

- **Secure Password Management:** This includes vaults for safeguarding credentials and other sensitive corporate data. A staggering 86 percent of breaches involve stolen credentials.

- **Comprehensive Administrative Reports, Auditing, and Logging.**
- **Multi-Factor Authentication (MFA).**
- **End User Check-In and Check-Out for Privileged Accounts:** Examples include requiring a ticket number, just-in-time access, justification for check-out, and specifying the length of access time.

It is also extremely important for IT pros to choose solutions that are seamless to implement and use, and which reduce — rather than create — friction for teams working toward compliance. This allows them to focus on their organization's core security objectives and obligations, rather than spend an enormous amount of time and effort trying to knock down silos and put out fires.

RISK #4

THE WORSENING RANSOMWARE THREAT

According to the *Devolutions State of IT Security in SMBs in 2023/24 Survey*, ransomware is the top cyberthreat that SMBs are concerned about — and this is not surprising. Consider these chilling numbers from Sophos' *State of Ransomware 2024 Report*:

- In the last year, 59 percent of organizations were targeted by a ransomware attack.
- 70 percent of ransomware attacks resulted in data encryption.
- 32 percent of ransomware victims whose data was encrypted also had data stolen.

- The average initial ransom demand has surged to $2 million.
- 34 percent of ransomware **victims** took more than a month to recover.

What's more, the UK-based National Cyber Security Centre (NCSC) has issued a warning that the global ransomware threat is expected to rise **due to advancements in AI**, which will increase both the volume and impact of ransomware attacks over the next two years.

WHAT IT PROS CAN DO TO PREVENT RANSOMWARE ATTACKS

Ransomware will remain a major threat for years (and probably decades) to come. However, IT pros can and must take steps to reduce their risk. The Center for Internet Security (CIS) recommends the following 15 actions:

1. **Create a Comprehensive Incident Response Plan:** Identify what to do in the event of a ransomware attack, and specify who should do it (and when).
2. **Implement a Backup System:** Ensure the backup supports multiple iterations or archived data. This is critically important in case one copy of the backup contains infected or encrypted files. Backups should also be regularly tested for data integrity and to verify operational readiness.
3. **Use Antivirus and Antispam Software:** Add a warning banner/signature on all emails to remind users about the dangers of clicking links and opening attachments.
4. **Disable Script Macros Where Possible:** Force end users to view rather than open files transmitted through email. Embedding malware inside macros is a common tactic for ransomware attacks.

5. **Keep All Devices, Software, and Applications Fully Updated and Patched:** This includes cloud locations. Using a centralized patch management system is recommended.

6. **Use Application Whitelisting and Software Restriction Policies:** These block the execution of programs in common ransomware locations (e.g., temporary folders).

7. **Use a Proxy Server for Internet Access.**

8. **Use Ad Blocking Software.**

9. **Restrict Access to Common Ransomware Vectors:** Examples include social networking sites and personal email accounts.

10. **Implement the Principle of Least Privilege (POLP):** Limit user permissions to only what is necessary for their job roles.

11. **Implement Network Segmentation and Zero-Trust Architecture:** Separate sensitive data and critical systems to minimize the damage from potential breaches.

12. **Assess and Monitor Third Parties:** Ensure third parties with network access follow all cybersecurity best practices.

13. **Participate in Cybersecurity Information Sharing Programs:** Examples include MS-ISAC and InfraGard.

14. **Provide End Users with Ongoing Cybersecurity Training:** Topics should include social engineering, phishing, and spotting signs of video and audio deepfakes.

15. **Implement a Reporting Plan:** Clearly inform end users how and when to report unusual or suspicious activity.

RISK #5

FACING FINANCIAL RUIN AFTER A CYBERATTACK

> All successful cyberattacks are destabilizing and costly. But for SMBs, the risk can be far greater. A report by IBM and the Ponemon Institute found that the average data breach cost for SMBs has climbed to a whopping $2.98 million per incident. **Separate research indicates** that 6 in 10 SMBs fold within six months of an attack. In other words, SMBs risk not just losing sales, savings, customers, market share, and reputation — they risk losing everything.

WHAT IT PROS CAN DO TO PREVENT RANSOMWARE ATTACKS

IT pros should use the recommendations described throughout this white paper to guide their cybersecurity efforts and serve as a checklist. Granted, due to budget constraints, many SMBs will not be able to take action on everything (e.g., implementing AI-powered deepfake detection systems). However, there are still several fundamental measures that should be part of the strategy and plan, including:

- Enforcing the **Principle of Least Privilege (POLP)**, zero trust, and network segmentation.
- Using a robust password manager.
- Training and testing end users.
- Deploying a PAM solution to monitor and govern privileged accounts.

THE ROLE OF CYBERSECURITY INSURANCE AND PAM SOLUTIONS

Speaking of PAM, many organizations are turning to cybersecurity insurance as a way to hedge against the potentially catastrophic costs of a breach. In response, a growing number of insurance providers are demanding that PAM controls **be** in place as a pre-condition of coverage. Generally, at a minimum, these insurers want proof of the following:

- **MFA for Remote Access:** Either through built-in functionality or integration with third-party tools (SMS-based MFA is being phased out due to the volume of successful SIM-swap attacks).

- **Updated Default Administrator Accounts and Configurations:** This prevents cybercriminals and rogue insiders from exploiting commonly available credentials.

- **Removal of Local Administrator Rights:** This is required on desktops/laptops, as well as **proper management of** local workstation accounts.

- **Timeouts for Remote Access Sessions:** Sessions should only remain open for as long as necessary to complete tasks.

- **Replacing Ultra-Powerful Administrator Accounts:** Instead, use multiple privileged accounts that establish specific permission requirements for each system administrators must access.

In addition to the above, some insurance companies require that policyholders have more advanced PAM controls in place, including:

- **Authentication Options:** Such as number matching for all users (not just privileged users).

- **Check-Out Capabilities:** Including built-in approvals to minimize who can request access to a privileged account, and for how long.

- **Just-in-Time (JIT) Privilege Elevation:** Converts previously high-privilege accounts into zero-standing privilege accounts.

- **JIT User Provisioning:** Privileged accounts are created as needed for a specific duration and are removed when tasks are completed.

THE FINAL WORD

The cyberthreat landscape is volatile, and predicting anything with rock-solid **certainty** is rarely a good idea — things change on a monthly, weekly, and sometimes even daily basis. However, it can be said without qualification or hesitation that IT pros who (along with their colleagues) embrace and apply the recommendations in this white paper will significantly strengthen their cybersecurity profile **and** materially reduce their risk.

IT pros in SMBs might do even more than this: their cybersecurity efforts, leadership, and vigilance could make the difference between whether their organization stays safe and thrives in 2025 — or is victimized by a major attack, which **could result in the organization disappearing entirely**. The stakes truly are this high, and they are only getting bigger.

LEARN MORE AND DIVE DEEPER

Devolutions offers a suite of solutions that help IT pros address and mitigate all of the risks discussed in this white paper by enforcing PAM, establishing network segmentation, safeguarding passwords, enabling session recording, and more. In addition, our solutions are affordable for SMBs that typically do not have large IT security budgets. They also integrate rapidly and seamlessly **into** the environment, support compliance requirements, and increase end user productivity, efficiency, and day-to-day work experience.

To learn more and dive deeper, email **sales@devolutions.net** and request a consultation to discuss your cybersecurity challenges and goals. Discover how our solutions **can** help you establish visibility and control, reduce risk, meet compliance requirements, boost end user productivity, and move your organization ahead!