ISSUE 97 | FALL 2023

BIZGROWTH STRATEGIES

IDEAS TO HELP YOUR BUSINESS COMBAT CYBERTHREATS

CYBERSECURITY SPECIAL EDITION

How Cybercriminals Are Weaponizing Artificial Intelligence

Employee Benefits Cyber Risk Exposure Scorecard

Closing the Security Gap: Managing Vendor Cyber Risk

Retirement Plan Sponsor Cybersecurity Checklist

Protect Your Digital Frontline With Employee Training

CBIZ
YOUR TEAM.

In This Issue

CBIZ.com

CBIZ

CBZ

CBIZServices

To subscribe to this newsletter or a variety of others, click here.

You can also call us at **1-800-ASK-CBIZ** (1-800-275-2249).

DISCLAIMER: This publication is distributed with the understanding that CBIZ is not rendering legal, accounting or other professional advice. This information is general in nature and may be affected by changes in law or in the interpretation of such laws. The reader is advised to contact a professional prior to taking any action based upon this information. CBIZ assumes no liability whatsoever in connection with the use of this information and assumes no obligation to inform the reader of any changes in laws or other factors that could affect the information contained herein.

Cyberattacks have emerged as one of the most significant threats facing organizations of all sizes. They're becoming more frequent and sophisticated, making recovery increasingly difficult.

Without proper preparation, these attacks can have devastating operational, financial, legal, reputational and cultural impacts, such as business disruptions, revenue loss, attorney fees and damages, and panic among employees and clients.

As cybercriminals continue to advance and evolve, a stagnant cyber risk management approach is simply not an option. Further, the prevalence of cyber breaches means cybersecurity is not solely an IT concern. It takes a robust set of processes and people from across your organization, working together toward a common goal.

Our professionals have developed these articles and resources to help you protect your organization from cyberthreats in multiple operational areas.

How Cybercriminals Are Weaponizing Artificial Intelligence

Artificial intelligence (AI) popularity has skyrocketed, captivating the interest of individuals and organizations. While offering numerous benefits, AI can be weaponized by cybercriminals. Discover how cybercriminals exploit AI technology and get protection tips for your organization.

Cybercriminals Harnessing the Power of AI

CREATING & SPREADING MALWARE

Cybercriminals traditionally utilize sophisticated technical skills to create malicious code and deploy malware attacks. AI allows cybercriminals with varying technical expertise to easily launch malware incidents. Other AI malware examples include:

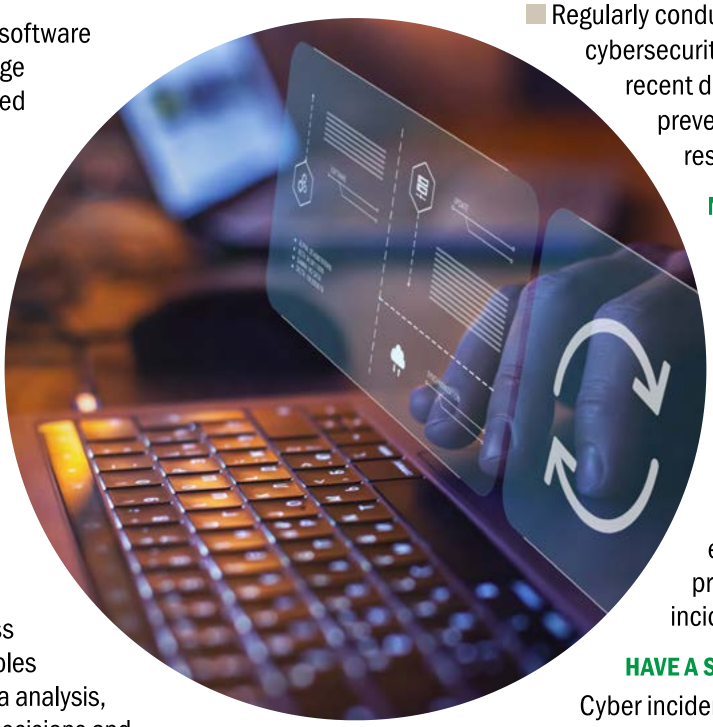
- Generating videos for downloading popular software
- Streamlining and automating different attack phases
- Assisting in identifying potential targets and personalizing ransom demands

CRACKING CREDENTIALS

Cybercriminals employ brute-force methods to expose password information and access to victims' accounts. AI is manipulated to systematically test word combinations to crack passwords.

SOCIAL ENGINEERING SCAMS

AI empowers cybercriminals to create credible phishing emails. Additionally, AI can modify a cyberattacker's facial and physical features to resemble someone the victim knows.



DIGITAL VULNERABILITIES

Cybercriminals typically seek software vulnerabilities they can leverage (e.g., unpatched code, outdated security) when infiltrating a network or system. Utilizing AI technology allows cybercriminals to uncover a broader range of software weaknesses, creating more opportunities for launching attacks.

STOLEN DATA

Cybercriminals examine stolen data for illegal actions, including selling the information, publicly disclosing and demanding ransom payments. This process is time-consuming, but AI enables cybercriminals to expedite data analysis, enabling them to make quick decisions and accelerate the attack execution. Consequently, targets have less time to detect and counter these attacks.

Defending Against Weaponized AI Technology

AI technology is expected to increase cyberattack frequency and severity. To safeguard operations and mitigate cyberthreats, you must stay updated on AI-related advancements and take proactive defense measures.

GOOD CYBER HYGIENE

Implement standardized routines to ensure the secure handling of workplace data and interconnected devices. These practices can safeguard networks and data against potential AI cyberthreats. Essential elements of cyber hygiene include:

- Immediately patching known vulnerabilities
- Discontinuing the use of unsupported software/systems
- Enforcing robust passwords, which should consist of a minimum of 12 characters and a combination of uppercase and lowercase letters, symbols and numbers
- Implementing multifactor authentication (MFA) enterprisewide
- Backing up data in a dedicated and secure location (e.g., air-gapped external hard drive, the cloud)
- Implementing firewalls, antivirus software and other relevant security programs on workplace networks and systems
- Regularly conducting employee cybersecurity training to educate them on recent digital vulnerabilities, attack prevention measures and incident response protocols

NETWORK MONITORING

Employ automated threat detection technology to conduct ongoing scans of digital ecosystems for potential vulnerabilities or suspicious activities. Such technology typically generates alerts upon the detection of security issues, enabling businesses to promptly identify and address incidents.

HAVE A STRATEGY

Cyber incident response plans can establish procedures to mitigate cyberattack damages. These plans must be thoroughly documented and regularly practiced, encompassing a range of potential cyberattack scenarios.

SECURE INSURANCE PROTECTION

Ensure appropriate insurance coverage to safeguard against potential financial losses resulting from the weaponization of AI technology. Seek guidance from a trusted insurance broker to assess and discuss your specific coverage needs. Selecting the broker and cyber carrier is a critical component of protecting your data as most carriers also require robust cyber risk management tools and 24/7 monitoring.

As AI technology continues to advance, so will its contribution to rising cyberattack frequency and severity. By keeping updated on the latest AI-related advancements and taking proactive measures to safeguard against its potential weaponization, you can keep your operations secure and ward off looming cyberthreats.

Connect with a member of our team for additional tips and coverage solutions.

Employee Benefits Cyber Risk Exposure Scorecard

During open enrollment, a high volume of extremely sensitive employee data is passed through various systems, software and teams. To protect this benefits data and other confidential information within your organization, it's essential to have the proper cybersecurity measures in place ahead of time.

Fill out our interactive scorecard to determine your current level of cyber risk exposure and learn what your score means at the end.

QUESTIONS	YES	NO	UNSURE	SCORE
Does your organization have a wireless network, or do employees and clients access your internal systems from remote locations?	□	□	□	
Does anyone in your organization take company-owned mobile devices, such as laptops, smartphones and USB drives, with them – either home or while traveling?	□	□	□	
Does your organization use cloud-based software or storage?	□	□	□	
Does your organization have a "bring your own device" (BYOD) policy that allows employees to use personal devices for business use or on a company network?	□	□	□	
Does your organization have critical operational systems connected to a public network?	□	□	□	
Does anyone in your organization use computers to access bank accounts or initiate money transfers?	□	□	□	
Does your organization digitally store the personally identifiable information (PII) of employees or clients?	□	□	□	
Has your organization ever failed to enforce policies around the acceptable use of computers, email, the internet, etc.?	□	□	□	
Can the general public access your organization's building without the use of an ID card?	□	□	□	
Is network security training for employees optional at your organization?	□	□	□	
Can employees use their computers or company-issued devices indefinitely without updating passwords?	□	□	□	
Has your IT department ever failed to install anti-virus software or perform regular vulnerability checks?	□	□	□	
Can employees dispose of sensitive information in the event of a system failure or other network disaster?	□	□	□	
Would your organization lose critical information in the event of a system failure or other network disaster?	□	□	□	
Can employees easily see what coworkers are doing on their computers?	□	□	□	
Has your organization neglected to review its data security or cyber security policies and procedures within the last year?	□	□	□	

TOTAL SCORE: 0

If you scored 20-32: While you've scratched the surface of cybersecurity prep, there's much more to be done to ensure that your organization's crucial data is adequately protected.

If you scored 7-19: You've started the process of prepping for a potential cyberattack, but there is more to be done to protect your employees' and clients' sensitive data.

If you scored 0-6: It's clear you've put careful thought and consideration into cybersecurity ahead of open enrollment. You've taken the necessary precautions to mitigate the risk of a cyberattack while also preparing an action plan should an attack occur. Keep it up!

Connect with an advisor to discuss how you can amp up your benefits-related cybersecurity.

Closing the Security Gap: Managing Vendor Cyber Risk

In today's interconnected business landscape, companies often rely on multiple vendors for services, from software to supplies, adding layers of cybersecurity risk. The $85 billion outsourcing industry offers cost savings, which benefits many organizations, but a vendor's lack of robust cybersecurity can expose a company's sensitive data to breaches. And, while many organizations invest in internal cybersecurity protection, they forget the risk extends to third-party vendors.

Best Practices for Third-Party Vendor Cyber Risk Management

A recent report reveals startling statistics about cybersecurity and third-party vendors: Only 13% of organizations continuously monitor the security risks associated with their external partners. Meanwhile, a separate report indicates that 98% of organizations worldwide are integrated with at least one third-party vendor that has suffered a breach in the past two years. These figures highlight a significant security gap in vendor cyber risk management.

Here are three cybersecurity risk management tips to consider:

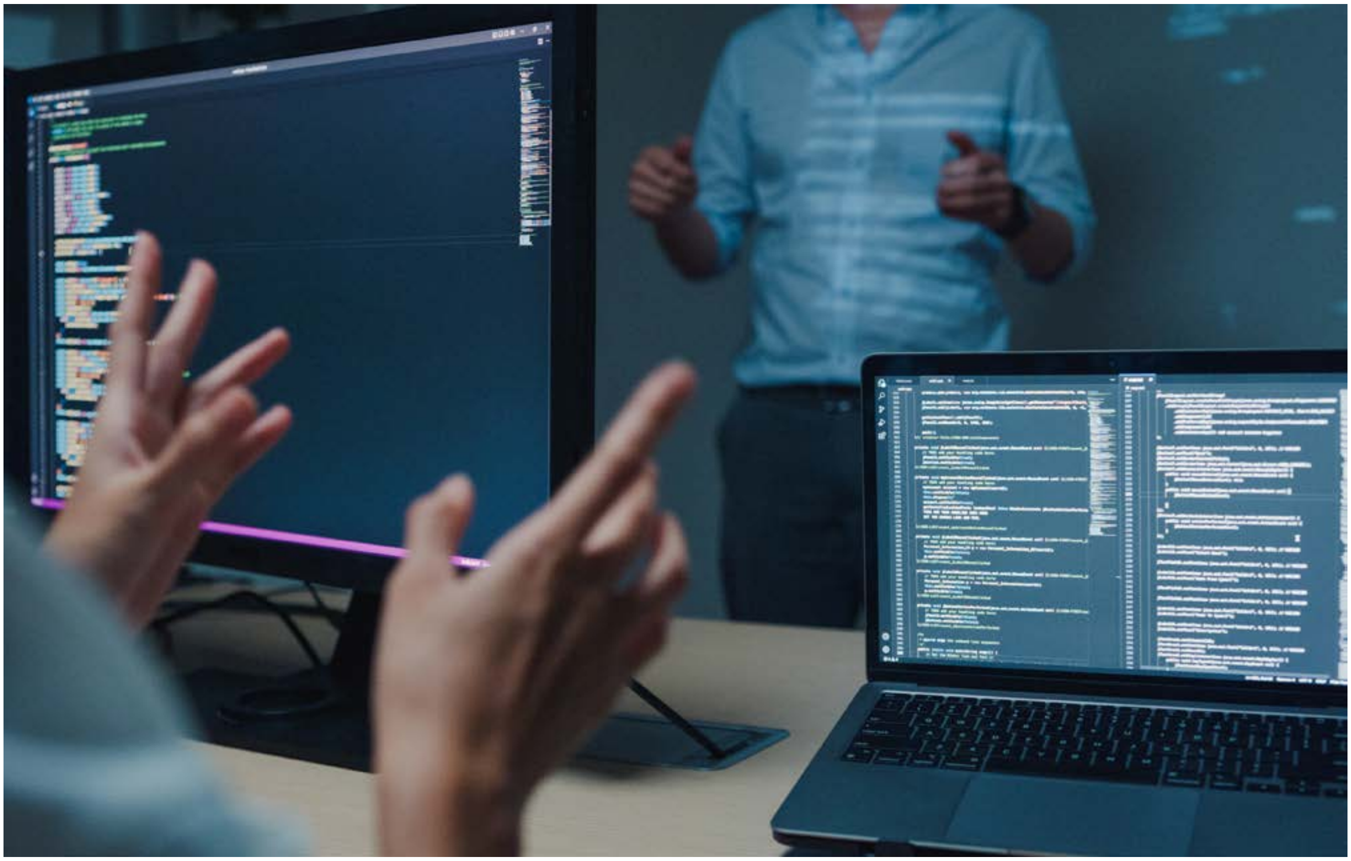
Understand the Risks Associated With Utilizing the Vendor

Conducting a thorough risk assessment is crucial before entering into a contractual agreement with third-party vendors. Examine the types of data the third party will have access to and familiarize yourself with their cybersecurity protocols.

Contracts with vendors should include specific security requirements and compliance standards. Ensure your agreement has clauses that permit regular security audits. It should also delineate responsibilities in the event of a data breach.

Remember that new risks can emerge even after performing due diligence at the onset of a vendor relationship. Maintain

(Continued on next page)



(Continued from previous page)

ongoing surveillance of your vendors' security posture. Utilize real-time dashboards, generate regular reports or continuously employ specialized third-party services to monitor vendor risk.

Verify the Vendor's Cybersecurity Program Effectively Manages Those Risks

This is most frequently done via "due diligence questionnaires." To streamline third-party risk management, vendors that provide third-party attestations like ISO 27001 or System and Organization Controls (SOC) reports can expedite and simplify the process. These reports provide independent validation of the security controls in place and help you identify any additional layers of suppliers. This level of detail provides greater visibility into your entire outsourcing and vendor web, helping you avoid potential blind spots.

Manage Your Risks Associated With Utilizing the Vendor

There are also simple steps your organization can take to mitigate risks. They include:

- **Incident Response Plan**: Have a clearly defined incident response plan that includes procedures for handling a breach involving a third-party vendor. Ensure the vendor understands your incident reporting requirements and their responsibilities in a security incident.
- **Employee Training**: Educate employees about the risks associated with third-party vendors and how to handle data responsibly. Many breaches happen due to human error or lack of awareness.
- **Limit Access**: Practice the principle of least privilege by only giving vendors access to the information they need to complete their tasks.
- **Contract Termination**: Ensure your contract mandates an orderly supported transition to a new vendor, including the return of all data in a structured, usable format.

By incorporating these practices into your vendor management programs, your organization can mitigate the risk associated with third-party vendors and enhance your overall cybersecurity posture.

Connect with one of our professionals to learn more.

— CYBERSECURITY SPECIAL EDITION —

Retirement Plan Sponsor Cybersecurity Checklist

With both retirement plan and DOL auditors assessing what plan fiduciaries are doing related to cybersecurity, it's important that plan sponsors and fiduciaries ensure that sufficient policies, procedures and processes are in place to protect systems and data.

The auditors could potentially ask for evidence and documentation related to a plan sponsor's due diligence and implementation of the appropriate cybersecurity safeguards, as well as communication to participants related to cybersecurity.

PLAN SPONSORS SHOULD CONSIDER THE FOLLOWING:

- □ Confirm status of employer cybersecurity insurance coverage, including whether they have it, what it covers and, more importantly, does not cover, as well as any fiduciary liability coverage.
- □ Perform periodic reviews of providers' cybersecurity policies and procedures and related cybersecurity program documentation to determine alignment with industry and security best practices and frameworks, and document and retain any pertinent results and recommendations as a result of the reviews.
- □ Request and review plan providers' documentation related to recent external security audits (e.g., SOC 2, ISO, HIPAA, NIST) performed by independent auditors or third parties.
- □ Confirm content, frequency and recipients of plan providers' cybersecurity awareness communication training.
- □ Inquire of plan providers regarding any past cybersecurity incidents and the related resolution and corrective actions.
- □ Understand the differences between the providers' cybersecurity and fraud protection policies.
- □ Confirm whether providers' service agreements contain any indemnification language that might apply to cybersecurity and/or fraud protection policies.
- □ Confirm with providers the number of participants who have never logged into the participant website and consider communicating cybersecurity risk to those participants.
- □ Confirm with record-keeper what communication is sent to participants related to cybersecurity, including the method and frequency of communication.
- □ Periodically communicate and educate employees directly on the importance of security best practices.
- □ Follow up with providers periodically regarding cybersecurity policies and procedures.
- □ Document all cybersecurity actions taken and decisions made.

Even if your retirement plan does not require an annual plan audit, plan fiduciaries should still conduct their internal reviews and cybersecurity due diligence activities, as the DOL may choose to randomly audit the plan and will likely look for this documentation.

Connect with one of our retirement and investment consultants to learn more.

Investment advisory services provided through CBIZ Investment Advisory Services, LLC, a registered investment adviser and a wholly owned subsidiary of CBIZ, Inc.

Protect Your Digital Frontline With Employee Training

No matter the business size, the opportunity for a cyber-attack is real. In fact, small to medium-sized businesses (SMBs) are proving to be more vulnerable than large businesses, as 61% of SMBs were targets of cyberattacks in 2021, making it critical for companies to boost their first line of defense through ongoing employee training.

Cybersecurity Basics

Creating a safe and secure cyber environment begins with understanding the basics of cybersecurity. A good place to start is by developing a policy document that clearly outlines the requirements and roles of each team member. This includes basic principles, such as password management, privacy settings and malware protection. It also means defining the education that employees need to properly identify threats and react appropriately when faced with suspicious behavior.

Employee Training

Training is essential to help protect against cyber threats. It's also a must for companies with cyber liability insurance, as policy documents often mandate employee training requirements that must be substantiated should a company ever experience a breach.

Companies should provide regular and relevant training beginning at onboarding. Staff should know about current and emerging attack trends and email phishing schemes. A solid understanding of cybersecurity basics can help team members better understand their role in defending against threats. Basic topics that should be covered include:

- Email phishing
- Secure passwords
- Safe internet browsing
- Social media
- Software installation & updates

Along with general knowledge, companies should also offer training programs focusing on the specific cybersecurity risks their business may face. Further, it's beneficial to conduct simulations, such as sending employees a phishing email, to see how they respond to potential threats.

Ongoing Training

Employee education will be an ongoing need as cybersecurity is an ever-evolving field and threats evolve daily. Businesses need to stay ahead of the curve, and more and more companies are accessing cost-effective strategies to keep staff informed. Learning management systems (LMS) offer access to an extensive library of engaging training programs that detail cyber safety policies, best practices and tips on spotting a phishing or malicious email and other potential threats.

An LMS can also ease the training burden while allowing real-time tracking and reporting that provides insights into employee learning progress. Such monitoring will be helpful if a company ever needs to substantiate its training program. It also aids in incentivizing teams to complete security tasks; this creates a culture of attentiveness that is key to creating a secure online environment. In addition, regularly scheduled cybersecurity-focused meetings can help keep the lines of communications open and employees updated on the latest risks and cybersecurity trends.

Businesses, regardless of their size, are vulnerable to numerous cybersecurity threats that can jeopardize their safety and reputation. It's crucial to have a comprehensive plan that includes providing regular cybersecurity training to employees and equipping them with the necessary tools and knowledge to defend against these threats. These elements are essential components of a strong cybersecurity framework. Thus, investing in cybersecurity training is no longer a choice but a requirement for companies to succeed and expand in today's digital world.

Connect with us to learn more about cybersecurity training.