EINPRESSWIRE

IT and Cybersecurity Goals to Keep an Organization Safe in 2024

If any of the following stats on cybersecurity concern you, here are eight keys to aiding an organization in facing increased cybersecurity threats.

SPOKANE, WASHINGTON, UNITED STATES, January 11, 2024 /EINPresswire.com/ -- Here are a few alarming statistics on cyber threats collected by Varonis.

Cyber fatigue, or apathy to proactively defend against cyberattacks, affects as much as 42 percent of companies. (Cisco)

97 percent of organizations have seen an increase in cyber threats since the start of the Russia-Ukraine war in 2022. (Accenture)

> Each individual has a role to play in defending an organization from cyberthreats. They need the training and tools to succeed,”
>
> *Heather Stratford, Drip7 Founder and CEO*

The average ransomware payout has increased dramatically from $812,380 in 2022 to $1,542,333 in 2023. (SC Magazine)
94 percent of malware is delivered by email. (Verizon)

Data breaches exposed more than 4.5 billion records in 2023. (IT Governance)[1]

There is no way for any organization to be 100 percent safe, 100 percent of the time in the digital world. Attacks are constant and growing in frequency and sophistication.

“Each individual has a role to play in defending an organization from cyber threats. They need the training and tools to succeed,” declared Heather Stratford, Drip7 Founder and CEO.

Here are eight actionable suggestions to incorporate in your 2024 plans.

Enhancing Employee Cybersecurity Training

Continuous education and training for employees on cybersecurity best practices, phishing awareness, and safe online behaviors are essential to create a security-conscious workforce. With the demand for skilled IT professionals growing, upgrading the skills of current employees can address the prediction by Gartner that by 2025, lack of talent or human failure will be responsible for over half of significant cyber incidents.[2]

Implementing MFA (Multi-factor Authentication)

Strengthening authentication mechanisms by incorporating multi-factor authentication across all systems and applications reduces the risk of unauthorized access, even if passwords are compromised. Microsoft reports that Microsoft systems deflect more than 1,000 password attacks per second, and more than 99.9 percent of compromised accounts don’t have multi-factor authentication enabled.[3]

Security Audits and Penetration Testing Scheduled Regularly

Conducting periodic security audits and penetration testing helps identify vulnerabilities and weaknesses in the infrastructure, applications, and networks, allowing for timely remediation. 73% of successful breaches in the corporate sector were carried out by penetrating web applications through their vulnerabilities.[4]

Assess and Address Third-Party Vulnerabilities

Third-party vendors, suppliers, and partners can introduce security risks, potentially compromising the overall security of an organization. Conduct thorough risk assessments of third-party vendors before onboarding them. Evaluate their cybersecurity practices, including data handling procedures, security measures, and compliance with industry standards and regulations. Establish clear security requirements in contracts with third-party vendors. Define expectations regarding cybersecurity standards, data protection measures, incident response protocols, and regular security assessments.

54% of businesses do not vet third-party vendors properly. According to a study, 48% of organizations deem third-party relationship complexity as their main problem.[5]

Incident Response Planning and Rehearsal, including Ransomware

Creating and regularly testing a comprehensive incident response plan enables a swift and organized response to security incidents, minimizing the impact of potential breaches.

The rise in ransomware attacks in 2023 further demonstrated the success of low-tech hacking techniques. Major firms, banks, hospitals and government agencies experienced a 51% increase in ransomware incidents. These attacks disrupted financial trading, caused shortages of essential products like Clorox wipes, and targeted critical infrastructure. However, due to the lack of transparency surrounding these incidents, reliable figures on the number of data breaches, the extent of the damage, and the hackers responsible remain elusive.[6]

Upgrade Password Practices

People and passwords are the weak link in many cybersecurity situations. Passwords play a fundamental role in cybersecurity. They serve as the first line of defense in protecting sensitive information, systems, and accounts from unauthorized access.

They should be long, complex, and include a combination of uppercase and lowercase letters, numbers, and special characters. Avoid easily guessable information like birthdays, common words, or sequential characters.

Reusing passwords across multiple accounts increases vulnerability. 81% of company breaches were caused by poor passwords. 80% of hacking incidents were caused by stolen and reused login information. 17% of hackers have successfully guessed other people's passwords.[7]

Regular software updates

Even the financial industry has been targeted by cyberthreats and made vulnerable by a lack of software updates.

A bug in cloud-networking software from NetScaler — a bug dubbed Citrix Bleed — led to disruptions at 60 credit unions, though no evidence suggests any data breaches resulted from the attack. However, Ongoing Operations, a credit union information technology firm, said it experienced a cybersecurity incident on November 26. Before the ransomware attack, Ongoing Operations had failed to patch a vulnerability in the NetScaler cloud-networking software, according to Kevin Beaumont, a cybersecurity researcher and former head of cybersecurity operations at the telecommunications company Vodafone.[8]

Social Engineering

Social engineering remains a significant threat to cybersecurity, exploiting human psychology to manipulate individuals into divulging confidential information, performing certain actions, or compromising security measures. Here are some common social engineering threats to be aware of: phishing, spear phishing, baiting, tailgating, impersonating, vishing, and waterhole attacks.

According to Bloomberg, the use of social engineering tactics by hackers is a notable trend. The hackers, Scattered Spider, employed deceptive phone calls to trick customer service representatives into revealing password credentials. Resorting to aggressive tactics, such as threatening employees with termination, the group managed to breach numerous organizations, including MGM Resorts International, Caesars Entertainment, and Coinbase. This aggressive, straightforward approach has resulted in about 52 breaches since 2022.[9]

Assess organizational cybersecurity defenses. Identify the vulnerabilities the organization needs to address. Create a plan with the people and resources needed to fill the gap. People are always the key. Implement a culture of vigilance, where employees feel comfortable and are even rewarded for reporting suspicious activities without fear of repercussions.

[1] https://www.varonis.com/blog/cybersecurity-statistics#:~:text=The%20global%20average%20cost%20of,percent%20higher%20than%20in%202022.
[2] https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cybersecurity-leaders-will-change-jobs-by-2025
[3] https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/
[4] https://www.getastra.com/blog/security-audit/penetration-testing-statistics/#:~:text=70%25%20of%20companies%20do%20penetration,pentest%20annually%20or%20bi%2Dannually.
[5] https://www.getastra.com/blog/security-audit/third-party-data-breach-statistics/#:~:text=27%25%20of%20all%20third%2Dparty,account%20for%2023%25%20of%20incidents.
[6] https://www.pymnts.com/cybersecurity/2023/simple-hacking-techniques-prove-successful-in-2023-cyberattacks/
[7] https://financesonline.com/password-statistics/
[8] https://www.americanbanker.com/list/6-of-the-biggest-threats-banks-faced-in-2023
[9] https://www.bloomberg.com/news/newsletters/2023-12-27/hackers-proved-in-2023-that-low-tech-methods-work-too

Deb McFadden
Drip7
PR@drip7.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram