Outsmarting Cybercriminals:
A Guide to Navigating Today's Cybersecurity Threat Landscape

Issued June 2024

TELARUS + SLY FOX SYSTEMS
1-844-531-7900

What's Inside Your Guide

SLY FOX SYSTEMS
1-844-531-7900

Introduction

To understand the 2024 cybersecurity threat landscape, open any news site. The headlines are filled with frightening tales of banks, internet service providers, healthcare organizations, and other big players suffering the costly consequences of growing cyberattacks. And even though they may not make it on the news, the local insurance broker, bookkeeping service, and pharmacy on the corner are not immune.

Key Statistics

- **2,365** cyberattacks and **343,338,964** victims in 2023.[1]
- **72%** increase in data breaches from 2021 to 2023. 2021 held the previous record.[1]
- US cybercrime costs reached approximately **$320 billion** as of 2023, expected to hit **$1.82 trillion** by 2028.[2]

The growing rate of cyberattacks creates a great deal of “FUD”: fear, uncertainty, and doubt. Many business owners ignore the risk to their organization and rely on hope and luck due to the complexity of cybersecurity. However, beginning a cybersecurity journey doesn’t need to be overwhelming. By viewing your organization from the perspective of an attacker, you can identify gaps and take action. In other words: Think like a bad guy.

In this guide, we will explore common cybercrime targets and how to help your organization outsmart costly intruders.

Understanding Common Cybercrime Targets

Even though it's against human nature, it's beneficial to examine your organization as a cybercriminal would. While it is always good to see the strengths of an environment, the bad guys are looking for the weaknesses. Here are some common cybercrime targets and ways to combat them:

1. Phishing and Untrained Staff

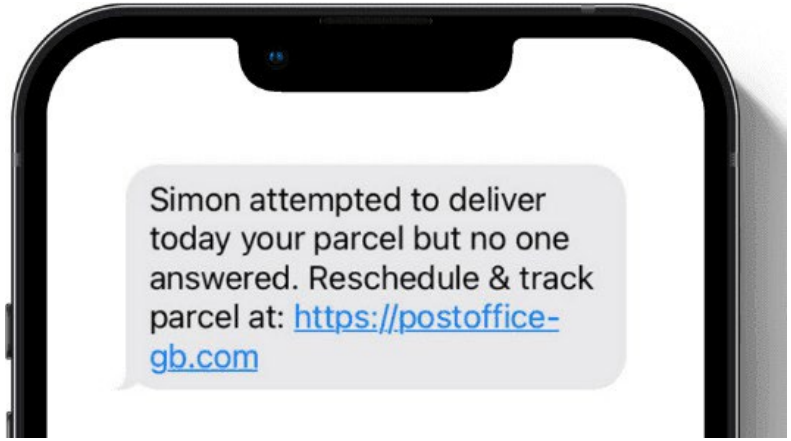
There is an adage that cybercriminals use: "We don't hack machines, we hack people." People are one of the weakest areas of an organization when it comes to cybersecurity. According to StationX, a leading provider of cybersecurity training and consulting, phishing is the most common form of cybercrime. Phishing involves sending scam emails or text messages that trick individuals into providing sensitive data or clicking malicious links. Over a trillion phishing emails are sent each year, and 36% of all data breaches involve phishing. [3]

Key Statistics

- **1 trillion+** phishing emails per year
- **36%** of all data breaches involve phishing

Combatting Phishing

Consider implementing cybersecurity awareness training that includes phishing campaigns. It is essential that employees are educated in the techniques that the bad guys use, especially phishing. Security staff should send random (but innocuous) phishing simulations to all employees at various times. When a link in one of these emails is clicked, the user should be educated on what happened and how to better respond the next time a suspicious message appears. These emails should not be used to embarrass or make fun of anyone but only to educate.



Tell-tale signs of a phishing message: Links that don't go to official websites. Do not be tempted to click!

2. Social Engineering and Unassuming Executives

CompTIA, a widely recognized IT trade organization, defines social engineering as “methods employed by hackers to gain the trust of an end user so that the hacker can obtain information that can be used to access data or systems." Social engineering typically involves impersonating representatives of legitimate organizations to manipulate people into supplying information such as passwords or personal details.[4]

Common examples include:

- **Spear-phishing:** Very targeted attacks against individuals within a business
- **Ransomware:** Malicious software which blocks access to a computer until a fee is paid
- **Pretexting:** Use of a fabricated story, or pretext, to gain a victim's trust and manipulate them into sharing sensitive information, sending money, etc.

Combatting Social Engineering

IT leaders need to take a close look at individuals within the company who have access to sensitive data, such as executive assistants, front office personnel, and helpdesk workers. Training them to recognize and not be afraid to question anything that doesn’t pass the “gut check” is critical. If these employees are hesitant, they should have the authority to escalate to management.

3. Cybersecurity Staff Shortages Create Unwanted Attention

CSO Online reports that the cybersecurity workforce shortage reached a record high of nearly 4 million, despite the cybersecurity workforce growing by almost 10% in the last year.[5]

This is a favorite "opportunity” of cyber criminals. All the bad guy needs to do is search their target company’s job boards and identify open IT and cybersecurity positions. The more positions that are open and the older they are signal a staff shortage, and possibly an effortless way to make entry.

Combatting Staff Shortages

While solving workforce shortages can seem daunting there are many service providers that will take this headache on for your organization. Service providers can monitor systems 24/7, reducing the burden and cost of maintaining internal staff and infrastructure. Additionally, the capital costs involved in creating a Security Operations Center (SOC) and training staff to a level needed to discover, respond, and recover from today’s increasingly complex incidents can add up.

4. AI-driven Cyber Threats and the Struggle to Keep Up

There is no doubt that the rise of artificial intelligence (AI) has taken the world by storm. While AI can do wonders for efficiency and productivity, the bad guys are using it in just as many ways for evil.

Among the most malicious applications: Cybercriminals use AI to create deepfake voices and impersonate corporate executives. CNN recently reported that a finance worker at a multinational firm was tricked into paying out $25 million to fraudsters who used deepfake technology to pose as the company's chief financial officer in a video conference call.[6]

Combatting Deepfakes

While deepfake technology is one of the most difficult attacks to counter, certain human elements cannot be forged. An effective way to outsmart deepfake videos or audio is to ask a question only the real person would know. For instance, if the target recently had dinner with the colleague the bad guy was imitating, they could ask a question about the restaurant, or the appetizer served. Simple human interactions like these can confuse even the most realistic forgeries.

Cybercriminals are also using AI to create new and harmful malware. This AI can test itself against security software to evade detection and find weaknesses in target systems, which cybercriminals use to plan and launch their attacks. This means that the malware can change its tactics during an attack, reacting to what it encounters to evade security measures more effectively. Additionally, "Dark LLMs", the criminal version of ChatGPT, can break into systems and spread malware. These tools are often sold on the dark web, making malware invasions and other cybercrime more accessible and harder to predict.

Combatting AI-driven Malware

Adopt a multi-layered security approach that includes employing advanced machine learning detection technologies, strong encryption and multi-factor authentication, and maintaining diligent software updates. Regular security awareness training and a robust incident response plan are also crucial.

Cybersecurity Threats and Recommendations Checklist

By following these recommendations, you can significantly improve your cybersecurity posture and better protect your organization against modern threats.

1. Phishing and Untrained Staff

Threat: Phishing involves sending scam emails or text messages that trick individuals into providing sensitive data or clicking malicious links. Understand that there are so many phishing attempts for one reason – because they work!!

Recommendation:

- Implement regular, ongoing cybersecurity awareness training, focusing on phishing techniques.
- Conduct simulated phishing campaigns to educate staff on identifying and responding to phishing attempts.
- Ensure that employees understand not to disclose sensitive information via email or text without verification.
- Provide an avenue for all employees to report suspected phishing attempts to the appropriate party.

2. Social Engineering

Threat: Social engineers manipulate people into providing confidential information. Examples include spear-phishing, ransomware, and pretexting.

Recommendation:

- Train employees, especially those with access to sensitive data, to recognize social engineering tactics.
- Encourage employees to verify identities and question requests that seem suspicious. Ensure that questioning these requests is expected and will be appreciated, even if the request is a valid one.
- Empower employees to escalate concerns to management if they feel something is off. Management should also have an avenue to report attempts, especially since management itself is a key target.

3. Cybersecurity Staff Shortages

Threat: Cybercriminals exploit workforce shortages in IT and cybersecurity departments, identifying them as weak points.

Recommendation:

- Consider outsourcing to managed security service providers (MSSPs) to monitor systems 24/7.
- Invest in automation and advanced security to alleviate the burden on limited staff.
- Develop a robust recruitment and retention strategy to fill critical cybersecurity positions.

4. AI Driven Cyber Threats

Threat: Cybercriminals use AI to create deepfake voices, videos, and advanced malware, making it easier to deceive and infiltrate systems.

Recommendation:

- Adopt multi-layered security measures, including advanced machine learning detection technologies.
- Implement strong encryption and multi-factor authentication (MFA) across all systems. New technologies also include the use of “passwordless” identity and authentication methods to verify users, utilizing biometric, environmental, and other data to confirm the identity of users.
- Regularly update software and conduct security patches on equipment to address vulnerabilities.
- Train employees to verify identities through personal knowledge questions that AI cannot replicate.

5. General Recommendations for Enhanced Cybersecurity

- **Risk Assessment**: Regularly perform comprehensive risk assessments to identify and address vulnerabilities.
- **Incident Response Plan**: Develop and maintain a robust incident response plan to quickly address and mitigate security breaches.
- **Third-Party Security**: Ensure third-party vendors and service providers adhere to stringent security standards and practices.
- **Continuous Monitoring:** Implement continuous monitoring of network traffic and user activity to detect and respond to anomalies in real-time.
- **Policy and Procedure Updates**: Regularly update cybersecurity policies and procedures to align with evolving threats and regulatory requirements.

SLY FOX SYSTEMS
1-844-531-7900

Conclusion

As more people conduct activities online and attacker techniques become more sophisticated, cyber threats have reached unprecedented levels. Ignoring these evolving threats will not reduce your organization's attack surface; inaction will only make it more attractive to the attackers. It's essential to prioritize security preparedness by honestly assessing your company's risks, addressing them promptly, and recognizing that some aspects may require external help.

You're not alone in navigating cybersecurity. Let's talk about how we can protect what matters most to you—today.

Click on the link to schedule you FREE 30 call

https://outlook.office.com/owa/calendar/SlyFoxSystemsSales@slyfoxsystems.com/bookings/?ismsaljsauthenabled

SLY FOX SYSTEMS

1-844-531-7900

SLY FOX SYSTEMS

is an MSP focused on strategy, technology and business transformation. Started by experts in cybersecurity and business processes, Sly Fox has grown organically to become a firm focused on bringing value to your entire organization by aligning technology with business strategy. Let us help you realize your business goals.

SLY FOX SYSTEMS

1-844-531-7900

TELARUS

Telarus, a premier global technology services distributor, has devoted over two decades to driving technology advisor impact and growth through deep market insights and experience, a partnership focus, and a comprehensive set of services, solutions, and tools. With a focus on collaboration with advisors and suppliers, Telarus enables technology advisors to source, purchase, and implement the right technology for the greatest impact.

www.telarus.com

Sources

1. St. John, Maria. Forbes: *Cybersecurity Stats: Facts And Figures You Should Know.* 28 February 2024. <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#Sources?>.
2. Statista. *Estimated annual cost of cybercrime in the United States from 2017 to 2028.* 17 July 2023. <https://www.statista.com/forecasts/1399040/us-cybercrime-cost-annual>.
3. Smith, Gary. *Phishing Statistics.* 10 April 2024. <https://www.stationx.net/phishing-statistics/>.
4. CompTIA. *What is social engineering.* N.d <https://www.comptia.org/content/articles/what-is-social-engineering>.
5. Hill, Michael. CSO Onine: *Cybersecurity workforce shortage reaches 4 milion despite siginficant recruitment drive.* 31 October 2023. <https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html>.
6. Chen, Heather and Kathleen Magramo. CNN: F*inance worker pays out $25 million after video call with deepfake 'chief financial officer'.* 2 April 2024. <https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>.
7. Telarus. *2023 Telarus Technology Trends Report.* <https://www.telarus.com/resources/tech-trends-2023/>.

SLY FOX SYSTEMS
1-844-531-7900