Bank of Botetourt

February 2024

Insider Threats: Mitigating Internal Cybersecurity Risks in the Finance Sector

The financial sector plays a pivotal role in the global economy in an increasingly digitized world. As financial institutions embrace digital transformation to provide more efficient and convenient services, they also face mounting challenges to safeguard customer data, prevent cyber threats, and adhere to stringent regulatory standards. Balancing innovation with security has become a core concern, making robust cybersecurity and compliance measures paramount.

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

The Intersection of Cybersecurity and Compliance

The financial sector continues to be a prime target for cyberattacks due to the potential financial gain from breaches and the cascading effects on customers, markets, and economies. Simultaneously, regulatory bodies have heightened their scrutiny, imposing rigorous requirements on financial institutions to ensure data protection, operational resilience, and overall system security.

Regulatory Landscape

Global regulatory bodies, such as the Financial Stability Board (FSB), Basel Committee on Banking Supervision (BCBS), and the General Data Protection Regulation (GDPR) in the European Union, have established frameworks to enforce cybersecurity and data protection standards. Additionally, country-specific agencies like the Federal Reserve, Office of the Comptroller of the Currency (OCC) in the United States, and the Financial Conduct Authority (FCA) in the United Kingdom are crucial in setting guidelines for financial sector cybersecurity.

Key Regulatory Standards

1. *ISO 27001:* This international standard systematically manages sensitive information and encompasses risk management, security policies, and incident response planning.
2. *NIST Cybersecurity Framework:* Developed by the National Institute of Standards and Technology (NIST), this framework offers a comprehensive set of cybersecurity guidelines and best practices to manage and reduce cybersecurity risks.

Continued on Page 2

Connect with us!

(540) 591-5000

3. *SWIFT Customer Security Programme (CSP):* For institutions engaged in SWIFT transactions, the CSP outlines mandatory and advisory controls to protect the confidentiality and integrity of customer data.
4. *Payment Card Industry Data Security Standard (PCI DSS):* Relevant to organizations handling credit card transactions, PCI DSS outlines security measures to protect cardholder data and prevent fraud.

Implementation Challenges

Meeting these regulatory standards presents unique challenges for financial institutions:

1. *Rapid Technological Advances:* The pace of technological evolution requires financial institutions to adopt and implement new security measures quickly.
2. *Complexity of Infrastructure:* Large institutions often have intricate and interconnected IT systems that demand coordinated security measures.
3. *Third-party Risk:* Collaborations with vendors and third parties can expose financial institutions to vulnerabilities outside their immediate control.

Compliance Benefits

While achieving compliance might be daunting, the benefits are manifold:

1. *Enhanced Reputation:* Meeting regulatory standards enhances the organization's reputation, fostering customer trust and loyalty.
2. *Reduced Financial Impact:* Compliance reduces the risk of data breaches, minimizing potential financial losses and legal repercussions.
3. *Operational Resilience:* Strong cybersecurity practices enhance operational resilience, ensuring uninterrupted services and reduced downtime.
4. *Competitive Edge:* Compliance demonstrates a commitment to security, potentially giving an institution a competitive advantage in the market.

5 Strategies for Success

1. *Risk Assessment:* Identify and evaluate potential cybersecurity risks and vulnerabilities specific to your organization.
2. *Holistic Approach:* Develop a comprehensive cybersecurity strategy that aligns with regulatory requirements and encompasses people, processes, and technology.
3. *Continuous Monitoring:* Implement ongoing monitoring and assessment to detect and respond to emerging threats promptly.
4. *Employee Training:* Train employees on cybersecurity best practices and their roles in compliance.
5. *Collaboration:* Foster collaboration with industry peers, regulatory bodies, and cybersecurity experts to stay informed about the latest threats and mitigation strategies.

Conclusion

The financial sector's journey toward cybersecurity and compliance is a continuous evolution. As technology evolves, so do cyber threats. Financial institutions must remain agile, adopting adaptive cybersecurity measures while meeting regulatory standards to ensure the safety and trust of their customers, stakeholders, and the global economy. By embracing innovation with security at its core, the financial sector can navigate these challenges and build a resilient and secure future.

Remember, cybersecurity is not just a legal requirement; it's an ethical responsibility to protect the assets and interests of all stakeholders in the financial ecosystem.

Sources/Credit:
Article:
Mark Arnold , Lares.com
Images:
Image by Pete Linforth from Pixabay,
Image by Cliff Hang from Pixabay,
Attribution: Pixabay, Pixabay Content License Summary

Top 10 Internet Safety Rules & What Not to Do Online

With more users accessing the Internet through mobile devices, the risk of scams, identity theft, and physical harm are changing and growing quickly.

Even though apps loom larger in most people's daily online interactions than traditional websites do, that does not mean that the basic Internet safety rules have changed. Hackers are still on the lookout for personal information they can use to access your credit card and bank information.

Unsafe surfing can also lead to other threats—from embarrassing personal comments or images that, once online, are nearly impossible to erase, to getting mixed up with people you'd rather have had nothing to do with.

Here are the Top 10 Internet safety rules to follow to help you avoid getting into trouble online (and offline).

1. Keep Personal Information Professional and Limited

Potential employers or customers don't need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn't hand purely personal information out to strangers individually—don't hand it out to millions of people online.

2. Keep Your Privacy Settings On

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. Web browsers and mobile operating systems have settings available to protect your privacy online. Major websites also have privacy-enhancing settings available. Make sure you have enabled these privacy safeguards, and keep them enabled.

3. Practice Safe Browsing

You wouldn't choose to walk through a dangerous neighborhood—don't visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware.

4. Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection

Corporate cybersecurity experts worry about "endpoints"—the places where a private network connects to the outside world. Your vulnerable endpoint is your local Internet Wi-Fi connection. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before providing information such as your bank account number.

To further improve your Internet browsing safety, use secure VPN connection (virtual private network). VPN enables you to have a secure connection between your device and an Internet server that no one can monitor or access the data that you're exchanging.

5. Be Careful What You Download

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. Don't download apps that look suspicious or come from a site you don't trust.

6. Choose Strong Passwords

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember, which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.

7. Make Online Purchases From Secure Sites

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections.

8. Be Careful What You Post

The Internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original does not remove any copies that other people made. Don't put anything online that you wouldn't want your mom or a prospective employer to see.

9. Be Careful Who You Meet Online

People you meet online are not always who they claim to be. Fake social media profiles are a popular way for hackers to cozy up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

10. Keep Your Antivirus Program Up To Date

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

Sources/Credit:

Articles:

Kaspersky

Image:

Image by Jan Vašek from Pixabay; Image by Gerd Altmann from Pixabay; Attribution: Pixabay, Pixabay Content License Summary