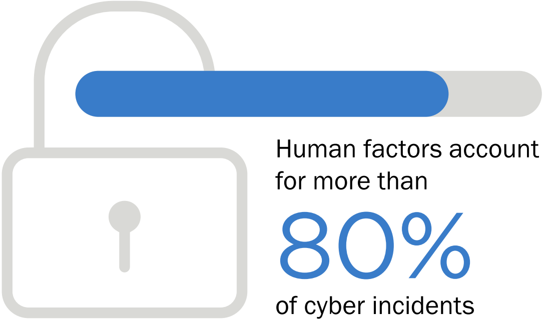
CYBER

Building a Human Firewall: Strengthening Your Cybersecurity Defenses

Building a Human Firewall: Strengthening Your Cybersecurity Defenses

Cyber threats are escalating. Reports from IBM show that cyberattacks using stolen or compromised credentials surged by 71%, year-over-year in 2023, and 32% of cyber incidents involve data theft and leaks. This indicates a shift towards stealing and selling data rather than encrypting it for ransom. The human element is often the weakest link in cybersecurity risk management. Creating a “human firewall” can significantly fortify your business against these threats. To better understand this concept, let’s explore the human factors that play a crucial role.



Human factors account for more than 80% of cyber incidents

Cybersecurity human factors

Research from Stanford University and Tessian shows that human factors account for more than 80% of cyber incidents. Common human errors include:

- **Social engineering:** Criminals trick employees into revealing confidential information.
- **Clicking malicious links:** Often found in phishing emails, these links can expose your systems to viruses, give threat actors access to confidential information, and compromise your organization’s security.
- **Bypassing security protocols:** For convenience, employees may ignore essential security measures.

For example, Change Healthcare faced a major data breach due to employees bypassing multi-factor authentication (MFA). Hackers accessed sensitive patient data, resulting in significant financial and reputational damage. One effective strategy to reduce risks such as these is implementing a human firewall.

What is an example of acting as a human firewall?

Turning your staff into diligent defenders against cyber threats can make a huge difference. Here are two real-world examples that illustrate the effectiveness of a human firewall in different sectors:

Financial Sector

The Royal Bank of Scotland reduced phishing incidents by 78% after implementing comprehensive employee training programs.

Healthcare Sector

A hospital network successfully defended against ransomware by regularly educating staff on recognizing phishing attempts.

Understanding cognitive and cultural drivers in cybersecurity

Building an effective human firewall also involves understanding the cognitive and cultural factors that influence employee behavior.

Cognitive aspects

Employees often take the path of least resistance, making decisions that prioritize convenience over security. This behavior is influenced by cognitive biases and the pressure to meet performance goals.

Organizational culture

A strong security culture balances responsiveness with skepticism. For instance, encouraging employees to verify suspicious emails can prevent many attacks. In the example, the company failed to enforce MFA and neglected security patches. Their culture prioritized convenience, leading to a significant data breach and Senate testimony from its CEO.

Changes to organizational structure

Key events affecting your organizational structure could also heighten the risk of human error. For example, with a merger or acquisition, the combination of different tech platforms, systems, and cultural norms could complicate cybersecurity practices.

Conduct thorough due diligence to assess the cybersecurity posture of acquired entities. Develop strategies to maintain security amidst organizational changes, such as standardized protocols and continuous monitoring.

Short staffing and burnout

Shortages in cybersecurity staff can impact risk management. Implement 24/7 monitoring using AI and analytics to continuously monitor systems. Prevent cybersecurity and IT team burnout by rotating shifts to ensure adequate rest periods and offering professional development opportunities to keep staff engaged and motivated.

Understanding the cultural and behavioral factors is an important next step, but it doesn't go far enough. The next step is adoption and implementation by your people.

Cybersecurity employee training

Providing regular and effective training is a cornerstone of maintaining robust cybersecurity. Engaging methods, such as animated modules, can improve employees' memory and understanding of the material. Implementing analytics to track training effectiveness and employee compliance further strengthens the training program.

Employee training is also important in the context of cyber insurance, as many insurers require organizations to have a baseline level of employee cybersecurity training in place to qualify for coverage. Proof of training can also reduce premium rates. Demonstrating a commitment to cybersecurity through regular training activities indicates to insurers that a business is taking proactive steps to mitigate risks. This proactive approach can lead to lower premium rates as it reduces the likelihood of costly claims.

A cadenced training system and setting a "tone from the top" are great places to start. For example, Risk Strategies conducts monthly cybersecurity training announced by the Chief Information Security Officer (CISO). This executive-led approach has proven effective in fostering a security-conscious culture.

Technological and procedural measures in cybersecurity

While regular and effective training is important, complement this with robust technical and procedural measures to ensure comprehensive cybersecurity. Some of these measures include:

- **Multi-factor authentication (MFA):** Adds an extra layer of security.
- **Strict password policies:** Enforce the use of complex passwords.
- **Vulnerability scanning:** Use AI-powered solutions to regularly scan for and address vulnerabilities, helping you detect and squash threats effectively.
- **Incident response plans:** Ensure comprehensive plans are in place for quick action during an incident.

Cybersecurity and human factors risk assessment and regulatory landscape

It's difficult to know the degree of human error your organization may be exposed to without conducting a cybersecurity and human factors risk assessment. This will help you gauge any gaps in the system and identify areas for proactive improvement. Here are some places to start:

Consistent self-auditing and optimization

Identify weaknesses in your systems, processes, and human behaviors that could be exploited by cyber criminals. Considerations may include weak passwords, lack of security awareness training, and susceptibility to phishing attacks.

For each identified risk, estimate the likelihood (probability) of it occurring and the potential impact (financial, operational, reputational) if it does. Use a risk scoring system to prioritize the most critical risks that need immediate attention.

Use tools for comprehensive assessments

Cybersecurity risk assessment tools help businesses identify and manage potential security threats. Popular tools scan for vulnerabilities, assess compliance risks, and analyze networks, applications, and devices to find weaknesses.

Some tools provide ratings based on security performance. Using these tools helps companies protect sensitive data and improve their overall security.

Keep up with evolving regulations and ensuring compliance

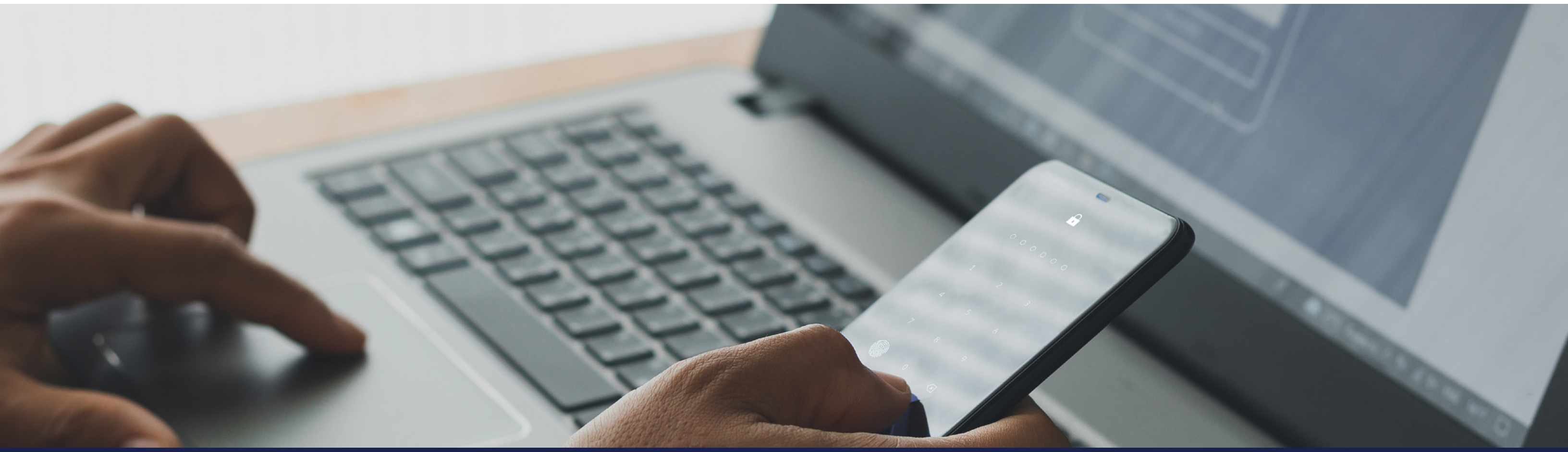
The US regulatory landscape for cybersecurity has become stricter over the last decade. Major laws like the Cybersecurity Information Sharing Act (CISA) encourage sharing threat information. The General Data Protection Regulation (GDPR) impacts US businesses handling European data. The National Institute of Standards and Technology (NIST) framework helps organizations improve their cybersecurity practices. Recently, the Cybersecurity Maturity Model Certification (CMMC) requires defense contractors to meet specific security standards.

Many insurance carriers now require vulnerability scanning before finalizing cyber insurance to ensure that businesses have addressed any potential weaknesses. The assessment is an important step for organizations to take before signing on for cybersecurity insurance.

Integration of AI in cybersecurity

In addition to assessments and compliance, integrating AI into your cybersecurity strategy can boost your defenses. AI can enhance cybersecurity by detecting phishing attempts, identifying anomalies, and reducing risks. Consider AI as a supplementary tool, providing an additional layer of protection by identifying suspicious activities that we, as humans, might miss.

While AI implementation can be costly, its benefits in preventing breaches could outweigh the initial investment. For example, AI can recognize phishing trends and block suspicious emails, reducing human error and enhancing overall security.



Future-proofing cybersecurity: the role of advanced technologies and human factors

The integration of advanced technologies, continuous improvement in training tools, and evolving cultural practices will continue to shape the future of cybersecurity risk management. Future AI tools will better recognize and block sophisticated threats, further reducing human error.

To effectively defend against cyber threats, focus on building a human firewall. This involves investing in employee training, implementing robust technological measures, and fostering a strong security culture. Stay updated on evolving trends and best practices to ensure your business remains resilient against cyber threats.

Want to learn more?

ABOUT RISK STRATEGIES

Risk Strategies is the 9th largest privately held U.S. brokerage firm offering comprehensive risk management advice, insurance and reinsurance placement for property & casualty, employee benefits, private client services, as well as consulting services and financial & wealth solutions. With more than 30 specialty practices, Risk Strategies serves commercial companies, nonprofits, public entities, and individuals, and has access to all major insurance markets. Risk Strategies has over 200 offices including Atlanta, Boston, Charlotte, Chicago, Dallas, Grand Cayman, Kansas City, Los Angeles, Miami, Montreal, Nashville, New York City, Philadelphia, San Francisco, Toronto, and Washington, DC.

The contents of this report are for general informational purposes only and Risk Strategies Company makes no representation or warranty of any kind, express or implied, regarding the accuracy or completeness of any information contained herein. Any recommendations contained herein are intended to provide insight based on currently available information for consideration and should be vetted against legal and business needs before application.