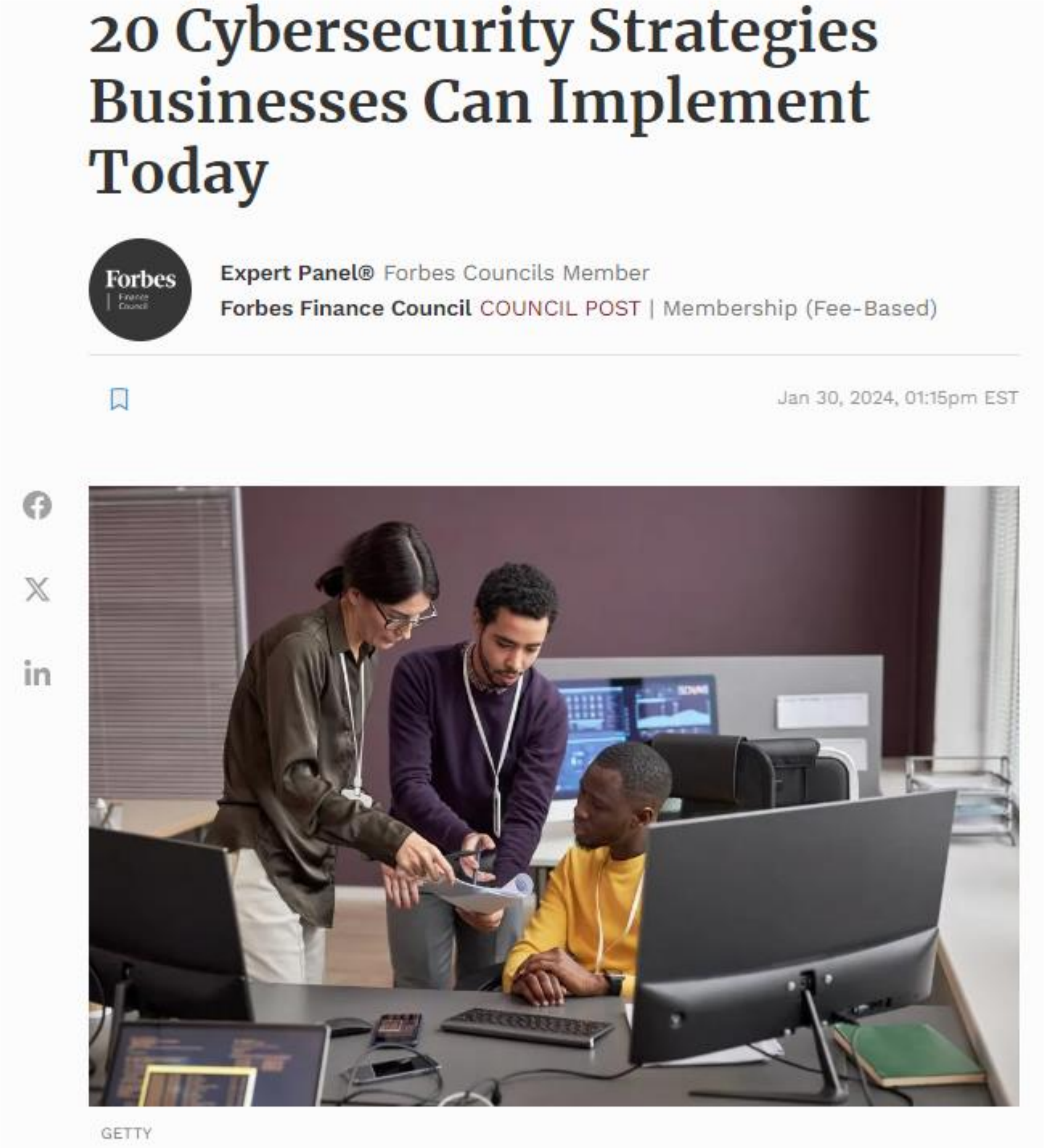
Forbes



20 Cybersecurity Strategies Businesses Can Implement Today

Expert Panel® Forbes Councils Member
Forbes Finance Council COUNCIL POST | Membership (Fee-Based)

Jan 30, 2024, 01:15pm EST

GETTY

As financial transactions and data storage increasingly shift to online platforms, the vulnerability to cyber threats is multiplying. For businesses, this means the implementation of robust cybersecurity measures is more important than ever.

Below, Forbes Finance Council members share 20 cybersecurity strategies business leaders should implement to safeguard their digital financial ecosystem. From regular security audits to comprehensive employee training, these practices can help protect against the growing sophistication of cyber attacks.

1. Hire An In-House Compliance Officer

As a Fintech CEO working with leading banks, there is a responsibility to protect sensitive information as we are obligated to comply with rules and regulations. We recommend having an in-house compliance officer, constantly keeping up to date with changing regulations, investing in the most secured software and making sure all processes within the company are compliant with ISO, SOC2 and GDPR requirements. - Tomer Guriel, ezbob Ltd.

2. Raise Awareness About Cybersecurity Threats

It is imperative to regularly convey the threats posed by cyber-attacks, as well as provide appropriate mitigation training to effectively respond to and prevent such threats. In addition, a meticulously crafted and thoroughly tested business continuity plan should be established to safeguard against disruptive consequences in the event of an imminent attack. - Charles Owo, Groupe SEB

3. Take Fraud Defense Measures

As more customers are acquired online, the risks of business identity theft and other forms of digital fraud rise. Fraud defense happens by attempting to improve existing tools or partnering with a powerful third-party solution provider. By leveraging data to offer instant decisions and credit, you strengthen the buyer-seller relationship and maintain a strong track record for risk decisioning. - Brandon Spear, TreviPay

4. Create And Maintain Contingency Plans

The question isn’t whether your company will face a cyber attack, it’s when it will occur. No matter how secure your systems are, cybercriminals will uncover a vulnerability. Companies need to establish and regularly review their contingency plans and understand where and how backup is happening. In addition, maintaining hard copies of critical documents is key to restoring lost data when needed. - Marc Blythe, Blythe Global Advisors, LLC

5. Balance Data Use And Security

It's important to strike a balance between utilizing data to drive intelligent and integrated experiences for customers and protecting the data. To strike the balance, data controllers should stick to three principles: 1. Less is more, focus on the data you need; 2. Don't be afraid to ditch dead data and 3. Embrace tech tools that help identify security risks before the data is compromised. - Fiona Roach Canning, Pollinate

6. Have A Communication Plan

Assume at some point you will be breached—most companies will. While identifying and stopping threat actors is a priority, having a well-designed plan for how, when and what you communicate with your customers will be critical to creating trust that will help you navigate a crisis. - Michelle DeBella, JumpCloud

7. Manage The Problem Collaboratively

First is the acknowledgment that cyber risks, like other risks, must be managed by all process owners and solved collaboratively. Key controls to consider on a bang-for-your-buck basis: multi-factor authentication with FIDO-compliant biometrics, email authentication (DMARC and BIMI) and good old-fashioned data hygiene and cyber hygiene. - Don Cardinal, Financial Data Exchange

8. Enhance Cybersecurity With AI Vigilance

Constant vigilance of cybersecurity controls through access control, network security, intrusion detection and remediation is essential. Careful analysis of how artificial intelligence (AI) can enhance a cybersecurity posture should begin. AI can supplement—but not replace—human judgment. Finally, understanding how AI could threaten your cybersecurity posture is key to managing threats. - Gale Simons-Poole, BHG Financial

9. Tighten Security With Encryption

Leaders should focus on robust encryption for safeguarding transaction data, multi-factor authentication to secure access and consistent employee training to prevent social engineering attacks. Additionally, ongoing monitoring and updating of security measures are crucial to adapt to the evolving cyber threat landscape. - Matt Johner, BankLabs

10. Ensure Leadership Emphasizes Cybersecurity's Importance

An excellent cybersecurity culture is paramount in protecting individuals and organizations. Core to an effective culture is understanding that the people of an organization are the most important protection, not technology. Installing such a culture begins with leadership. It is the responsibility of the chief executive to ensure employees understand the threats against cybersecurity. - Rupert Lee-Browne, Caxton

11. Have Strategies And Preventative Measures In Place

It's not a reasonable expectation to turn all your employees into cybersecurity experts. Adopt a mix of safety-net and prevention measures to stop threats from getting to your employees, and then alert and response knowledge measures, so teams know how to escalate issues to the experts fast. - Sabrina Castiglione, Pento

12. Ensure Employees Are Trained And Aware

The vast majority of cyberattacks originate from employee vulnerabilities. Employees can unknowingly create entry points for cybercriminals through their actions and behaviors making them a common target for cybercriminals. - Simone Grimes, Simone Grimes

13. Take A Multi-Faceted Approach

Cybercrime has become so prolific and sophisticated that it takes a multi-faceted approach today to safeguard your business. You need elements of all the following: proper technology, double authentication systems and processes, verbal authentication and authority on larger dollar transfers, cyber insurance and CPI (constant process improvement) to catch new threats. - Paul Daneshrad, StarPoint Properties

14. Create A Cyber-Resilient Business Culture

Business executives must create a cyber-resilient culture to navigate the intricacies of a changing digital financial ecosystem successfully. Use robust encryption software, conduct frequent security audits and ensure payment mechanisms are safe for sensitive data. Administer access controls, provide cybersecurity best practices training to staff and keep up with new threats. - Jared Weitz, United Capital Source Inc.

15. Implement Cybersecurity Education Programs

Employee awareness and training are pivotal in maintaining proactivity against cyber threats. From phishing threats to mobile and remote work security, just to name a few, the need to educate and train employees has never been more crucial to mitigating human-related vulnerabilities. Being vigilant in this effort will contribute to your organization's overall cybersecurity resilience. - Jeffrey Bartel, Hamptons Group, LLC

16. Maintain Open Communication With Employees

Fortinet research found over 80% of organizations experienced cyberattacks that target employees. To mitigate risk, companies should move beyond static defenses, embrace layered security, develop proactive threat intelligence and most importantly, implement employee cybersecurity awareness programs. Open communication and collaboration within the organization is the strongest defense. - Parth Kulkarni, Adobe

17. Involve Your Board of Directors

You can get the attention of your Board of Directors and involve them in an important company decision regarding your cybersecurity program. Cybercrime is an ever-increasing business risk. A cybersecurity effort must evolve yearly with a dedicated budget to defeat criminals. - Dave Sackett, Persimmon Technologies Corporation

18. Employ Password Protection

The simplest way for rogue actors to access corporate networks is through accidentally misplaced passwords. If a company has 200 employees and each employee uses four passwords, that’s 800 passwords being entered almost daily. If those 800 passwords are managed differently per employee, it’s a near certainty that at least one password will be accessible to outsiders. - Todd Sixt, Strait & Sound Wealth Management LLC

19. Secure Data Access Using Multi-Factor Authentication

Use multi-factor authentication (MFA) to add an additional layer of security between a hacker and sensitive financial information like financing details for investors. MFA ensures that users authenticate their personal identity, often with biometric data, before accessing sensitive information. Proper cybersecurity policies are a must for any organization entrusted with sensitive information. - Anthony Georgiades, Innovating Capital

20. Have Periodic Security Audits And Evaluations

As fire is the test of gold, implementing scheduled security audits and assessments (including internal, statutory and cyber audits) is a proactive measure in identifying vulnerabilities within the system. Consistently testing the infrastructure, applications and networks ensures the prompt identification and resolution of potential weaknesses.
- Pankaj Vasani, Cube Highways InvIT

Link to Forbes Article