



Authority Magazine

Cyber Defense: Natalia Gindler Corsini Of Prae Venire On The 5 Things Every American Business Leader Should Do To Shield Themselves From A Cyberattack



Authority Magazine Editorial Staff

Follow

12 min read · 5 hours ago





To establish a strong, consistent, and standardized approach to cybersecurity across an organization, leaders should implement an internal cybersecurity control framework. For example, investment firms manage sensitive financial data, client portfolios, and proprietary market strategies, making them prime targets for cybercriminals seeking to exploit system

vulnerabilities. It should be mandatory for such firms to adopt a cybersecurity control framework based on a recognized industry standard.

. . .

In our uncertain and turbulent world, cyberattacks on private businesses are sadly a common tactic of hostile foreign regimes as well as criminal gangs. Cyberattacks and ransomware have crippled large multinational organizations and even governments. What does every company need to do to protect itself from a cyberattack? In this series called “5 Things Every American Business Leader Should Do To Shield Themselves From A Cyberattack” we are talking to cybersecurity experts and chief information security officers who can share insights from their experience, with all of us. As a part of this series, I had the pleasure of interviewing Natalia Gindler Corsini.

Natalia Gindler Corsini is the founder and managing director of Prae Venire, a boutique corporate compliance consulting firm based in South Florida. With over 25 years of multinational experience in finance, international trade, ethics, and compliance, she specializes in helping U.S. companies operating abroad and foreign companies doing business in the U.S. Natalia holds an MBA in finance, controllership, and auditing from FGV in Brazil and is a Certified Fraud Examiner, offering tailored solutions in anti-corruption, internal controls, and corporate investigations.

. . .

Thank you so much for joining us in this interview series! Before we dig in, our readers would like to get to know you. Can you tell us a bit about how you grew up?

I grew up in a country, Brazil, where threats, whether from crime or instability, were a constant part of daily life. Over time, people adapt, and what might seem alarming elsewhere becomes part of what's considered "normal." Living in that environment, I developed a heightened sense of awareness early on. Without even realizing it, my alert system was always on. That upbringing naturally shaped my perspective and, little by little, led me to pursue professional paths focused on risk and fraud management. As I advanced in my career and studied the evolving challenges companies face, from political and economic instability to technological disruptions, I became increasingly drawn to compliance work. Over time, it became clear that cybersecurity wasn't just an IT issue, but a critical part of any effective compliance program. Like HR, finance, procurement, or operations, it needs to be addressed through policies, procedures, training, internal controls, and monitoring. Growing up in a high-risk environment gave me the instincts, and compliance gave me the structure, to help organizations navigate risk more consciously and strategically.

Is there a particular story that inspired you to pursue a career in cybersecurity? We'd love to hear it.

I didn't pursue a career specifically in cybersecurity, as it naturally falls within the broader compliance framework. Compliance programs are designed to address issues that pose legal, financial, and reputational risks to organizations. Cybersecurity is one of those critical areas, not only because of legal obligations to protect individuals from harm, but also due to

the substantial financial and reputational risks it presents to organizations and their leadership. This isn't about a single incident; it's about the alarming rise in cybercrimes that are becoming increasingly common and complex. For instance, cybercrime networks have been linked to human trafficking operations, which Interpol estimates generate \$3 trillion in profits globally each year (<https://www.cnn.com/2024/03/28/asia/southeast-asia-interpol-scam-human-trafficking-crime-intl-hnk/index.html>). These crimes are often seen as lower risk than drug trafficking or extortion, making them attractive to organized crime groups. Additionally, cyber fraud cases, such as criminals impersonating employees from financial institutions to commit wire fraud, are on the rise. These are the kinds of threats compliance programs must now account for and actively combat.

Can you share the most interesting story that happened to you since you began this fascinating career?

In my compliance career, I once assisted a client who was in the process of implementing a compliance program focused on domestic and international anti-corruption laws. During one of our training sessions, an employee noticed something unusual happening with his computer. Long story short, hackers had taken a QR code from WhatsApp Web and embedded it on a malicious site. They lured the employee to this fake page and instructed him to scan the fraudulent QR code using WhatsApp. In Brazil, it's very common for people to use WhatsApp for business purposes, including sending and receiving professional and sensitive documents. Many access WhatsApp Web on their computers. This practice is especially prevalent in small, mid-sized, and family-owned businesses, where WhatsApp is used extensively. As a result, a significant amount of confidential information is mishandled via WhatsApp. People often justify this by pointing out that WhatsApp is encrypted; while encryption offers some protection, it doesn't fully

safeguard users if a hacker gains access to their phone or computer. In the end, I supported the company not only in developing anti-corruption internal controls but also in creating AI, communication, and text messaging policies and procedures.

You are a successful leader. Which three character traits do you think were most instrumental to your success? Can you please share a story or example for each?

Every step of my professional journey has involved navigating uncharted territory. I never stepped into a role with a roadmap already laid out, instead, I built it myself. Looking back, three traits were instrumental in shaping my success: resilience, patience, and emotional strength.

Resilience became my anchor during one of the most defining moments of my career. I was tasked with implementing the company headquarters' compliance program at a regional subsidiary, an environment that was openly resistant. Rather than retreat, I stood my ground, remained focused on the mission, and took a strategic, measured approach. Over time, I earned the headquarters' support and successfully rolled out the program.

Patience is critical in navigating the cultural and operational differences I encountered. Change doesn't happen overnight, especially in compliance. I have been learning to listen more than I speak, to let trust build gradually, and to discern when to push and when to pause. That patience helped me earn credibility in environments where compliance was initially seen as a hurdle rather than a value.

Emotional strength keeps me steady throughout. Facing adversity, isolation, and the pressure to compromise isn't easy. I must separate my emotions

from my responsibilities, remain composed under pressure, and stay focused on the bigger picture. That strength not only helps me endure challenging moments, but it also enables me to lead others through theirs.

These traits weren't learned from training manuals or formal education. They were earned through lived experience, each challenge, each unfamiliar assignment, and each situation where I had to learn from scratch. They're what empower me today to confidently navigate the ever-evolving world of compliance, no matter what new technologies, governments, or generations bring to the table.

Are you working on any exciting new projects now? How do you think that will help people?

I'm assisting a client in updating their compliance program to align with emerging trends in the field, with a stronger focus on AI compliance, export controls, and third-party management. In the area of AI compliance, the program will provide clearer guidance on preventing cyber fraud, along with communication and training to raise awareness about the risks of sharing sensitive information when using AI tools. It will also address the dangers of generating content with inaccurate information or relying too heavily on AI during recruitment processes, which can lead to unconscious bias and discrimination by HR. These initiatives will help people by protecting personal and sensitive information, reducing cyber fraud exposure, promoting fair and ethical hiring practices, fostering a culture of responsibility and awareness.

For the benefit of our readers, can you briefly tell our readers why you are an authority about the topic of Cybersecurity?

In my field, I specialize in implementing compliance in a practical and effective way, integrating it into employees' daily routines rather than creating a check-the-box system filled with legalese meant only for external display. AI and cybersecurity are essential topics that must be addressed in any compliance program. From a regulatory perspective, they are required by authorities; from an organizational and individual standpoint, they are vital for protection against significant legal, financial, and reputational risks.

Ok super. Thank you for all that. Let's now shift to the main focus of our interview. In order to ensure that we are all on the same page let's begin with some simple definitions. Can you tell our readers about the different forms of cyber attacks that we need to be cognizant of?

From an organizational perspective:

- **Phishing Attacks:** Deceptive emails or messages that trick employees into revealing sensitive information or clicking malicious links.
- **Ransomware:** Malicious software that encrypts company data and demands payment to restore access, often crippling operations.
- **Business Email Compromise (BEC):** Attackers impersonate executives or vendors to manipulate employees into transferring funds or sensitive data.
- **Distributed Denial-of-Service (DDoS):** Overloads a company's systems or website with traffic, causing downtime and operational disruption.
- **Third-Parties Vulnerabilities:** Infiltration through third-party vendors or software updates that compromise the broader corporate environment.
- **Credential Stuffing:** Use of leaked username/password combinations to gain unauthorized access to systems.

From an individual perspective:

- **Phishing and Smishing:** Email and SMS scams designed to extract personal or financial information.
- **Identity Theft:** Use of stolen personal data to open accounts, commit fraud, or access financial assets.
- **Social Engineering:** Tactics used to deceive individuals into disclosing confidential information, such as posing as IT support.
- **Malware and Spyware:** Harmful software downloaded through suspicious links that steal or monitor personal data.
- **Public Wi-Fi Exploits:** Interception of data on unsecured public networks by malicious actors.
- **Account Hijacking:** Unauthorized access to email, social media, or financial accounts used to steal data or scam contacts.

Who has to be most concerned about a cyber attack? Is it primarily businesses or even private individuals?

Based on the response above, it affects both.

Who should be called first after one is aware that they are the victim of a cyber attack? The local police? The FBI? A cybersecurity expert?

From a company standpoint, organizations typically have an IT team and a cybersecurity team, either internal or external, depending on the company's size, responsible for analyzing breaches, preserving evidence, and stopping further intrusions. These teams are the first to be contacted. Next, due to legal obligations, the legal team must be notified. They are responsible for

immediately reporting the incident to the appropriate agencies and authorities, such as the FBI and local law enforcement. Together with the legal team, the risk management and compliance teams come into play, ensuring that all protocols are followed properly. This includes issuing notifications to customers and stakeholders, who must be informed promptly.

From an individual perspective, the first point of contact is usually the affected institution, such as a bank, to help prevent further damage. However, in today's digital world, where most transactions are conducted online, I recommend that individuals also maintain contact with cybersecurity professionals who can act quickly to contain any breach. There are now several specialized firms offering these services to small businesses and individuals, and I believe they should be the first point of contact, followed by the relevant institutions. Simultaneously, incidents should be reported to agencies and local authorities (e.g., the FBI, local police).

What are the most common data security and cybersecurity mistakes you have seen companies make that make them vulnerable to ransomware attacks?

Failing to regularly update and patch software and systems leaves known vulnerabilities open to exploitation. Many companies still permit weak or reused passwords and do not enforce multifactor authentication (MFA). Employees often fall victim to phishing emails, the most common entry point for ransomware, due to a lack of regular training and simulated phishing tests.

Additionally, companies often neglect network segmentation or fail to maintain isolated, offline backups. Once ransomware infiltrates the system, it can encrypt everything, including backups, making recovery nearly impossible without paying the ransom.

Vendors and third-party partners may have access to internal systems without adequate oversight or access controls. Sensitive data may be stored or transmitted without encryption, while excessive user access, outdated or unnecessary sensitive data retention, and misconfigured cloud environments further increase risk.

Other common vulnerabilities include vendors mishandling customer or employee data, unprotected data on laptops or mobile devices, improper disposal of storage media or printed documents, insider threats, and sensitive data not being properly identified, secured, or monitored, especially in backups.

What would you recommend for the government or for tech leaders to do to help limit the frequency and severity of these attacks?

Cybersecurity resilience requires more than technical solutions, it demands a strong culture of compliance and internal control. While government efforts are already underway, more can be done. The Cybersecurity and Infrastructure Security Agency (CISA) leads national initiatives to protect critical infrastructure, promote cybersecurity best practices, and coordinate emergency communications. The Committee on Foreign Investment in the United States (CFIUS) plays a key role in safeguarding national security by reviewing foreign investments that could pose risks to U.S. interests.

Additionally, the Federal Trade Commission (FTC) and the Department of Justice (DOJ) have increased enforcement actions related to cybersecurity

practices and data breaches. On April 8, 2025, the DOJ's new data security rule went into effect, highlighting the growing link between geopolitical risk and cyber threats. A 90-day grace period was announced for companies to comply with new rules on foreign adversary access to U.S. sensitive data. The National Institute of Standards and Technology (NIST) also continues to support cybersecurity efforts through its widely adopted Cybersecurity Framework, which helps businesses manage and reduce risk. Despite these advances, gaps remain, particularly from a compliance and internal control perspective. While regulations often require "reasonable" or "adequate" cybersecurity measures, they typically lack prescriptive internal control frameworks. Mandating annual cybersecurity risk assessments could help companies stay proactive instead of reactive. Stronger third-party oversight is also critical, as many breaches originate from vendors that lack proper vetting. Mandatory employee training should include certified completion records and behavior improvement metrics. Cybersecurity remains too siloed under IT, when many breaches stem from compliance failures, such as poor policy enforcement, internal reporting weaknesses, or lack of governance. Organizations must be encouraged to integrate cybersecurity policies, training, and enforcement into their compliance programs. From a tech leadership perspective, adopting stronger internal compliance frameworks is essential. This includes implementing robust internal controls, embedding cybersecurity risk assessments into operational audits, conducting thorough third-party due diligence, launching comprehensive employee training, and establishing clear incident response protocols. As threats evolve, a unified strategy among regulators, businesses, and tech providers will be key to reducing cyber risk.

Ok, thank you. Here is the main question of our interview. What are the "5 Things Every American Business Leader Should Do To Shield Themselves From A Cyberattack" and why? (Please share a story or example for each.)

1 . To establish a strong, consistent, and standardized approach to cybersecurity across an organization, leaders should implement an internal cybersecurity control framework. For example, investment firms manage sensitive financial data, client portfolios, and proprietary market strategies, making them prime targets for cybercriminals seeking to exploit system vulnerabilities. It should be mandatory for such firms to adopt a cybersecurity control framework based on a recognized industry standard.

2 . Conducting regular cyber risk assessments helps identify vulnerabilities, track emerging threats, and ensure that security measures are continuously evolving. For example, e-commerce companies should frequently conduct cyber risk assessments to evaluate new technologies and systems. If a vulnerability is discovered in their payment gateway system, they can address the issue promptly, preventing a costly data breach before it occurs.

3 . Enforce strong third-party risk management to ensure that vendors are maintaining robust cybersecurity practices. For example, a financial services firm could require all its vendors to undergo annual cybersecurity audits and provide proof of compliance with the firm's internal cybersecurity standards. This ensures that any third-party companies handling sensitive data are adequately protected, reducing the risk of a breach due to weak vendor relationships.

4 . Mandate employee cyber hygiene training and awareness to help employees recognize and respond to cybersecurity threats, preventing common attack vectors. For example, a healthcare organization could implement quarterly cybersecurity training, where employees learn how to recognize phishing emails, handle sensitive patient data securely, and respond to security breaches. This training can drastically reduce the risk of employees inadvertently exposing the organization to cyber threats.

5 . Establish real-time incident detection and response protocols to quickly identify and contain threats, minimizing damage. For example, a tech company could set up a Security Operations Center (SOC) that monitors network traffic in real-time. If the system detects unusual activity, such as an employee accessing sensitive data at odd hours, an automatic alert is sent to the compliance and IT teams. This ensures immediate investigation and response, minimizing potential exposure from an attack.

You are a person of enormous influence. If you could inspire a movement that would bring the most amount of good to the most amount of people, what would that be? You never know what your idea can trigger. :-)

If I could inspire a movement that would bring the most benefit to the most people, it would focus on ethical leadership in cybersecurity. This movement would encourage business leaders to prioritize the protection of sensitive and personal data, invest in proactive security measures, and view cybersecurity not just as a technical necessity but as a core ethical responsibility. By fostering an environment of transparency, accountability, and continuous improvement, businesses and governments could mitigate risks, prevent cyberattacks, and protect individuals' privacy as well as national security, benefiting everyone.

How can our readers further follow your work online?

By accessing either my website or my LinkedIn profile

This was very inspiring and informative. Thank you so much for the time you spent with this interview!