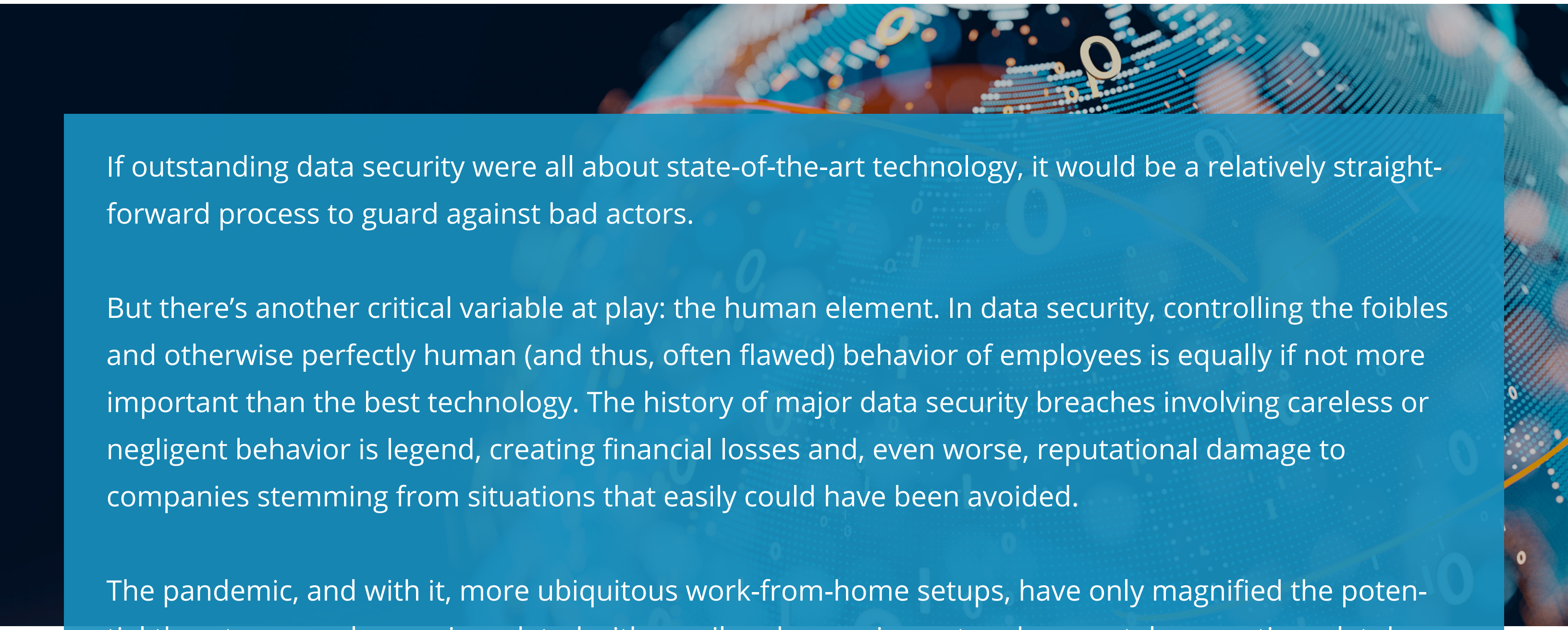
Data Protection in the Age of Cybersecurity Threats



If outstanding data security were all about state-of-the-art technology, it would be a relatively straightforward process to guard against bad actors.

But there’s another critical variable at play: the human element. In data security, controlling the foibles and otherwise perfectly human (and thus, often flawed) behavior of employees is equally if not more important than the best technology. The history of major data security breaches involving careless or negligent behavior is legend, creating financial losses and, even worse, reputational damage to companies stemming from situations that easily could have been avoided.

The pandemic, and with it, more ubiquitous work-from-home setups, have only magnified the potential threats as employees, inundated with email and accessing networks remotely, sometimes let down their guard. That’s why Gen II has moved toward a carefully calibrated security environment designed to neutralize many of the human errors commonly exploited by hackers. You could call it an enhanced data protection culture that effectively tightens human vulnerabilities while maintaining an in-depth defensive strategy.

Workplace procedures around cybersecurity and data breaches are changing. An evolving paradigm is “zero trust,” in essence, a set of protocols that takes nothing for granted and brings additional security steps that significantly reduce the opportunities for human-error breaches. It should be said that the lack of “trust” reflects more on error-prone people than bad intentions. It’s all about limiting the windows of opportunity for bad actors.

- Effective cybersecurity involves constant monitoring, training, testing, and vigilance — threats are a moving target and growing volumes of data makes it easier for them to hide. It is an ongoing, continual improvement process, not a one-off exercise. Gen II deploys state-of-the-art technology and regularly tests its network’s vulnerabilities and readiness through third parties.

- Gen II also trains its employees on proper cybersecurity behaviors as soon as they are onboarded and continually trains them to reinforce positive behaviors when it comes to cybersecurity and data protection. Monthly newsletters are sent via email on a different cybersecurity topic each month which helps to keep employees alert to the threats the company faces on an ongoing basis.

- Gen II also tests our employees’ susceptibility to phishing with monthly, anonymously sent emails. Our Security Analysts create well-designed phishing campaigns, and the results and metrics are reviewed by the Information Security Officer to understand gaps and ways to improve employees’ behavior to various phishing scenarios.

Controlling the trust factors

Hackers always seem poised to exploit undue trust, as was vividly demonstrated in a phishing exercise that cost one hedge fund nearly $6 million and spurred a lawsuit. As a result, personnel needs to be provided with systems, education, processes, and controls to satisfy service needs, while maintaining a high degree of security focus. Gen II has put careful controls in place, including:

- Multi-factor authentication for accessing the Gen II network.
- Carefully limiting data availability to those who need it. Gen II doesn't allow users to send attachments; Gen II doesn't allow users to print from home, where a lot of sensitive data can escape from hard copies.
- Virtual desktops and thin client laptops, which don't allow data to be stored on them – eliminating the classic stolen laptop breach.
- Aggressive password management, which is crucial to foiling hackers; one solution Gen II has implemented to reduce password knowledge by having employees enter banking and LP portals where they don't have access to the passwords.

Best-in-class cyber monitoring and protocols

Hackers always seem poised to exploit undue trust, as was vividly demonstrated in a phishing exercise that cost one hedge fund nearly $6 million and spurred a lawsuit. As a result, personnel needs to be provided with systems, education, processes, and controls to satisfy service needs, while maintaining a high degree of security focus. Gen II has put careful controls in place, including:

- Gen II SSAE 18 - (SOC) 1 Type 2 Compliant. Gen II has received an unqualified report on its control environment for 10 consecutive years. Gen II will have our SOC II Type I by the end of Q2 and expects to complete a SOC II Type II by the end of the year.
- Gen II strictly adheres to SEC Cybersecurity guidelines, CCPA, and the NY SHIELD Act
- Gen II conducts regular "stress-testing" to our infrastructure in the form of vulnerability and disaster recovery testing, vulnerability scanning, security incident tabletop exercises, and network penetration testing, all by third-party vendors.
- Gen II implemented the ISO 27001 ISMS framework throughout the company, a European standard that Gen II also utilizes in the U.S.
- Gen II uses AI to sort through the high volume of data for threats to our network and data assets. It's a technology that learns as it scans.
- Segregating one client's information from the other, not just externally, but internally within the business teams, is also important. Giving clients that assurance of data segregation with proper controls is paramount.

There's no underestimating the ingenuity of hackers, especially in financial services, where there's so much at stake. In a constantly evolving environment, Gen II brings the best possible defenses to bear. And yet our approach to data protection proves that increased employee flexibility, and access to data on the cloud, doesn't have to sacrifice security. That's why Gen II continues to make meaningful investments in personnel, process, and technology to ensure best cybersecurity practices and leverages the cloud, not just for systems and applications, but also for end user desktops.