The risk is real

As data becomes increasingly important in the asset servicing world, Jack McRae explores how different firms are bolstering their cybersecurity

Data is becoming more and more important for the asset servicing industry. As settlement cycles shorten, newer alternative assets are created, and AI takes its place at the top table, it is vital that firms can access and protect their extensive and accurate data. Yet, with its increased importance, data becomes a target and its golden value accepted not just by firms, but also by nefarious actors. As the asset servicing industry races towards an automated, digital world, cyber threat is at an all time high and the industry needs to be prepared.

Andrew Rose, chief security officer at SoSafe, believes that the industry is a "prime target for security threats" owing to its "highly digitalised environment, where employees regularly interact with technology and manage sensitive data."

This means that "cybercriminals understand that such industries present valuable opportunities, making them more susceptible to attacks." Rose explains. "The industry's close ties and dependencies with various entities in the supply chain further exacerbate its vulnerability, a concern that 80 per cent of security experts have noted as becoming increasingly apparent."

Rose points to a key combination of factors which would attract cyber threats — valuable data, frequent digital interactions, and susceptibility to social engineering.

So how does the industry better protect itself?

Data defenders

"Companies are continuously being attacked," says Nick Smith, global head of managed services at SmartStream, "Threat actors are continuously probing and looking for vulnerabilities to exploit and, when they do, they often sell this access to other threat actors to exploit."

The threat actors are constantly evolving and the industry has to be mindful to adapt with them. Smith believes that "serious investment" is needed to mitigate the threats which are set to "grow at an exponential rate".

Smith continues to warn that everyone is affected by cybercrime. He says: "It is not just financial services that are at risk. The global economy feels the shockwaves when a key component to the cyber security framework experiences an issue, as seen with the recent Windows issues following the CrowdStrike patch. The risk is real."

images by murrstock/stock.adobe.com

> ***The motivations for cyber attacks have expanded from being financially motivated to including market disruption, deception, and the demonstration of an element of power***
>
> **Jason Harrell, DTCC**

SoSafe's Rose reiterates the sentiment, explaining: "In an era where data is a critical asset, strong cybersecurity in the finance sector is indispensable. It protects against a range of threats, ensures regulatory compliance, and fosters trust — key factors for the stability and success of asset servicing operations."

He continues to argue that firms that prioritise bolstering their cybersecurity will be best positioned to "manage risks, maintain operational integrity, and secure their clients' assets in an increasingly digital and interconnected financial landscape."

Even with this investment, Rose urges firms to be extra vigilant. "While technical security measures are crucial, they alone are insufficient against the sophisticated tactics of modern cybercriminals," he adds.

Jason Harrell, managing director of operational and technology risk and head of external engagement, believes that failings in cybersecurity can lead to severe reputational damages. He explains how "these threats pose significant market risks and compromise a firm's reputation and trust. Ensuring comprehensive cybersecurity strategies, investing in employee training, and harnessing the power of emerging technologies bolster the capabilities and resilience that can safeguard the financial services sector."

The need for firms to defend their data is paramount but what are these threats?

The weakest link

For SmartsStream's Smith, "threat actors are driven by a variety of motives, but typically it is financial gain that is the objective."

He believes that while data is usually targeted, it is with the view of profiting from it. Smith notes: "We see different approaches once an environment has been breached. Threat actors will either lock a company out of their own data or they may steal the data in order to sell that same data elsewhere. Often the weakest link that causes the breach continues to be the human element."

DTCC's Harrell, however, believes threat actors are far more multifaceted and come in a variety of forms.

"Over time, the motivations for cyber attacks have expanded from being financially motivated to including market disruption, deception through misinformation and disinformation, and the demonstration of an element of power," He explains.

"Therefore, financial institutions can no longer view attacks solely based on 'stealing money'."

Looking forward, Harrell believes that "generative AI may also enhance the effectiveness of certain attacks, such as phishing, by allowing the adversary to create more realistic emails to convince users to conduct activities that subvert security controls. All of these trends will continue in 2025."

SoSafe's Rose points to research by Forrester that, "predicts that in 2024, 90 per cent of all cyberattacks will target human emotions. Commonly, despite being an age-old threat, these human focused attacks arrive via phishing emails as they continue to prove highly effective."

Rose explains how SoSafe have "identified the five most common attack types reported by companies as phishing, malware, Distributed Denial-of-Service (DDoS), ransomware, and broader social engineering attacks".

A key commonality between attacks remains data, according to Rose. He says: "In most cyber attacks, data is the primary target as attackers seek to steal, manipulate, or restrict access to sensitive information, such as personal details, financial data, or corporate secrets.

"This is often done to commit fraud, extort money — as in ransomware attacks — or gain unauthorised access to systems. Even in attacks not directly targeting data, such as DDoS, the ultimate goal can often be to disrupt access to data or services dependent on data."

No magic bullet

So how can cybersecurity improve to better protect key data? For SmartStream's Smith the solution is clear — evolution.

"Companies have to continuously evolve and refine their security frameworks," he explains. "With AI expanding its voice capabilities, threat actors have another channel to exploit and we now see companies developing fraud detection solutions to identify voice attacks driven by AI, as to the human ear the AI driven voice attack will sound just like the voice of a known individual."

Cyber threats' ever-evolving nature does make it difficult for firms to protect themselves and Smith stresses that no "single solution is the magic bullet", but rather firms will need to arm themselves with a full security framework.

Despite no magic bullet existing, all three industry figures believe that closer collaboration between the authorities and firms will help combat financial crime.

Smith believes that authorities should be doing more. He says: "The perception is that the authorities do relatively little in protecting companies, and when a company is being attacked the authorities contribute little value outside the requirement of having the attack reported to them.

"The media occasionally reports a threat actor network being taken down, but it feels like every day a major enterprise, health provider, financial institution, government agency finds itself a victim to an attack and faces financial commitments regardless of the path the entity elects to follow."

Smith continues to push for the severity of cyber attacks to be reported with greater urgency and concern.

He explains that these attacks "will impact the public whether they are aware of it or not. It may be that some companies are not able to survive an attack as nobody will do business with them — especially if the attack becomes public, which may impact the share price of a listed company, which then impacts the value of pension funds, or it may see an increase in insurance premiums with the additional costs being passed on to consumers."

DTCC's Harrell points to the 'standards' set by the authorities that offers a minimum level of "safety and soundness of the financial markets and strengthen protections against consumer harm". He continues to argue that the authorities are important in instilling trust within the services, however any degree of inconsistency in these 'minimum standards' can "create fragmentation in the frameworks used by financial institutions to manage cyber and other operational risks, resulting in an increased probability that controls across the institution are not cohesive".

Harrell believes that the best solution for the industry would be to continue to deliver a close alliance "between public and private partnerships between financial institutions, financial authorities, and standards bodies that drive regulatory coordination, decrease operational friction, and enhance the protection of information and information systems".

SoSafe's Rose is also complementary to the authorities, and labels their role "crucial" and their support "invaluable" in the broader cybersecurity landscape. Despite this, he also wants the regulatory bodies to do more. "Many regulations now rightly include the human factor as a key component of cybersecurity compliance," Rose begins. "However, these regulations often represent only the minimum standards necessary for compliance, which need to be significantly expanded to achieve true risk minimisation."

Rose also wishes for the industry to go beyond reliance on authoritative bodies to set standards for cybersecurity. He believes that there is a "pressing need for more unified reporting mechanisms and enhanced international collaboration to ensure a more cohesive and effective response to cyber threats".

Rose concludes: "While we greatly value the efforts of law enforcement and regulatory bodies, it's essential for firms to go beyond these minimum standards and proactively invest in comprehensive security measures. By fostering closer collaboration between the public and private sectors, we can create a safer digital environment for everyone." ■