LORCA NEEDS ACCELERATOR: FINANCIAL SERVICES

LORCA

The pandemic has placed pressure on global economies, aggravated geopolitical tensions and accelerated digital transformation. This is making the financial services sector a high-value target for hackers, activists and nation state threat actors.

As financial institutions (FIs) try to understand how they can thrive after the pandemic, they will encounter new geopolitical, socioeconomic, external technology and internal technology challenges.

For example, there is likely to be increased activity by nation state actors, hacktivists and organised crime groups, which will require FIs to re-evaluate the threat landscape. Organised crime groups are already becoming increasingly sophisticated and organisations are working hard to mitigate the impact of ransomware attacks.

With the pandemic driving the move to a cashless society and digital currencies become more popular, organisations will need to improve their ability to authenticate the use of their digital services and reduce online fraud.

Developments in AI and quantum computing also means firms will have to adapt their defences before these technologies are weaponised and pose a real threat.

Lastly, as banks pursue digital transformation initiatives, they will have to make sure that the cloud is secure, that they can gain assurance from suppliers and secure their remote workforces.

Lloyds Banking Group led the discussion as part of its commitment to cyber innovation in financial services. Our discussion unveiled these priorities:

1. Supply chain assurance.
2. Authentication of biometric identities.
3. Securing remote workers.
4. Increasing people's awareness of deepfake technology.
5. Implementing post-quantum cryptography algorithms.
6. Adopting new defences to ransomware attacks.
7. Reducing the reliance on cloud-managed service providers.

8 Implementing zero-trust architecture in the cloud.

9 Addressing security configuration in the cloud.

10 Adopting consequence-driven threat modelling.

11 Regulators need to update guidelines as threats and technologies evolve.

SUPPLY CHAIN ASSURANCE

Managing supply chain risks is a perennial problem for many organisations. One attendee commented that it's currently their organisation's main concern and they are looking to change their approach.

The crux of the problem is a lack of visibility over an ever-growing supply chain. Organisations use existing tools to implement governance, policy and controls and to identify threats in the supply chain in real time.

But despite continued monitoring, governance, active testing and periodic auditing of their suppliers, organisations still don't know if their third parties are implementing controls correctly. FIs don't feel that they have assurance that their suppliers are secure. Trust and transparency needs to be fostered across the supply chain.

Attendees mentioned that sharing experiences and raising awareness within the ecosystem could be a good defence mechanism. They observed that this already happens internally within departments and in shared intelligence groups, but not down the supply chain.

Other means of increasing supply chain assurance include promoting mutual due diligence through internal procedures and standards, creating incentives for third parties to assure themselves, raising the standard of cyber hygiene that suppliers have to meet and increasing the focus on supply chain internally by making supply chain due diligence, assurance and awareness a core function or capability.

AUTHENTICATION OF BIOMETRIC IDENTITIES

Biometric identification is being used more since the start of the pandemic. In some areas of financial services, biometric identification has become compulsory. For instance, one bank in Mexico will only allow people to open a bank account if they provide their fingerprint and in some American banks you need to provide your fingerprint to access services.

The challenge with using biometric identification is making sure that the right person is using the device. For instance, someone attempting to compromise an individual's mobile banking account may be able to change the settings on a smartphone so that the facial recognition software authorises the attacker's face.

Instances like this can occur because biometric data doesn't leave the device: it's the certificate that's stored centrally. While biometric identification works well for the most part, banks can't authenticate the user in instances like these.

As the UK moves towards a cashless society, biometric fraud is likely to increase. Multi-factor Authentication (MFA), which combines biometric identification and a secondary form of ID, could reduce this risk. But combining MFA and biometrics can increase friction at the point of sale or use by customers.

This means banks need alternatives that allow them to authenticate the use of biometrics, or MFA alternatives that decrease friction at the point of sale.

SECURING REMOTE WORKERS

Before the pandemic, banks relied on controls implemented in the workplace to reduce insider risk and data leakage. Working from home has meant that banks have less control over the environment of their staff. and given that the trend is likely to continue, banks need to regain control.

Attendees felt that they should be providing employees with more support and make sure that they're working from home securely. Some attendees felt that physical controls and securing hardware would be needed to reduce the immediate risks.

For instance, staff could be asked to use privacy screens or install a second router used solely for work purposes. However, these mitigations were seen only as a short-term solution that would not protect against malicious actors for long.

Organisations that began working from home before the pandemic have more mature practices for securing remote environments. These organisations are reluctant to monitor their employees as it can foster a culture of distrust. Instead, they have adopted the principles of zero trust and developed education, training and awareness programmes that focus on the benefits, risks and common problems associated with cyber hygiene.

These programmes acknowledge that most of the threat is due to negligence and use authorised guidance and the promotion of Cyber Essentials encourage high standards and a culture of continuous improvement.

INCREASING PEOPLE'S AWARENESS OF DEEPFAKE TECHNOLOGY

Deepfakes have been used to conduct social engineering attacks such as business email compromise attacks, as well as disinformation campaigns used to cause reputational damage. As the technology becomes increasingly available, the cost of using deepfakes is likely to decrease. Deepfake attacks may become more prevalent, meaning that organisations will need to increase their defences.

Deepfake disinformation campaigns are more common than deepfake social engineering attacks, so attendees believe that attacks causing reputational damage pose a greater threat. But they think that this is almost entirely out of their control.

Current methods for detecting disinformation include real-time alerting and threat intelligence for the propagation of campaigns. However, attackers can use automation to amplify the spread of their fake news, which means the organisation will always be in a reactionary position.

Attendees told us that having more control over the potential impact of a disinformation campaign would require organisations to increase the strength of their brand. Others also believe that the prevalence of fake news is so high that customers and external stakeholders may begin to distrust unfamiliar sources, which may naturally reduce the potential impact.

Some organisations intend to educate their customers, external stakeholders and employees about the technology. For example, one organisation intends to raise awareness by creating their own version of a deepfake attack. However, they haven't managed to get hold of the technology yet.

Attendees noted that instances of deepfake social engineering attacks have been successful in the wild because there is currently no established process for dealing with deepfake attacks. Regardless of the technology, humans are always the weakest link in these instances. This means organisations need to create processes to help employees navigate these threats.

Enforcing these processes may present challenges, and attendees believe that the first step to overcoming them would be to educate their staff. These training programmes would describe what a deepfake attack might look like, provide advice on how to identify an attack early on and give guidance on how to react.

IMPLEMENTING POST-QUANTUM CRYPTOGRAPHY ALGORITHMS

Quantum computing poses a threat to today's encryption standards because increased processing power would mean that current public key encryption techniques could be broken. As a result, the National Institute of Standards and Technology (NIST) is hoping to develop post-quantum cryptography (PQC) standards by 2022, which will likely come into effect in 2023-2025.

Attendees recognised the need to make the move to post-quantum algorithms, but stated that they have purposefully not invested in the move. FIs are reluctant to invest for a number of reasons. Firstly, they believe that this is a future threat that will not emerge for a number of years. Even if the threat emerges sooner than anticipated, an attacker would need to have the motivation, technology and expertise to conduct the attack. This makes a quantum attack unlikely.

Secondly, there is some doubt about the assurance of post-quantum cryptography, as PQC algorithms will need to undergo years of research to determine their reliability. The alternative is Quantum Key Distribution (QKD), which guarantees that a quantum channel cannot be intercepted successfully without detection. However, QKD requires specialised hardware, meaning that it's more costly to implement than PQC (which is software based). FIs would like to see more development and traction in this space before they invest in either option.

Lastly, NIST have not yet finalised their PQC standards. Making the move too early could be costly and result in FIs being locked into one algorithm.

Despite these reservations, FIs recognise that the result of a quantum attack could have a huge impact, so they intend to monitor developments closely.

ADOPTING NEW DEFENCES TO RANSOMWARE ATTACKS

Financial services is a high-value target for threat actors, and most FIs have seen an increase in the number and sophistication of ransomware attacks in recent years. The significance and efficacy of ransomware attacks has increased substantially with the advent of new technology, structured orchestration of attacks and ingenuity of organised crime gangs.

For example, Advanced Persistent Threat (APT) is now available as a service and organised crime groups are conducting reconnaissance around organisations' cyber insurance policy to understand how they should price an attack.

Attendees considered ransomware to be top threat for their organisation, so much so that some have established a team dedicated to understanding it and defending against attacks. These teams will seek to improve the defences of the ecosystem by looking for weak points or points of limited control certainty in third-party suppliers or managed service providers (MSPs).

Beyond increasing general cyber hygiene across the supply chain and increasing employee awareness and training, organisations are currently focusing their efforts on:

- evaluating their use of next-generation antivirus tools
- organising red team exercises that focus on ransomware intrusions
- arranging independent audits such as ransomware risk assessments
- looking at data vault solutions that increase their resilience to these attacks

Attendees would like authorities to make ransomware attacks illegal. They did recognise that this would be hard to implement and regulate as it would require the development of a robust framework and an advanced surveillance network where central authorities work closely with private organisations. This would be a huge undertaking, requiring a clear delineation of roles, responsibilities and liabilities and a system for reporting ransomware attacks.

REDUCING THE RELIANCE ON CLOUD-MANAGED SERVICE PROVIDERS

Security is a top priority for cloud migration, and many FIs have turned to MSPs and vendors to manage potential risks. These service providers need access to some company tools and data to deliver their services. FIs find that they need to act with caution when using MSPs as they need to make sure that they have secure and sound data privacy policies.

Meanwhile, as more services are steadily moved to the cloud, more service providers and vendors are being engaged. The proliferation of cloud-based tools across an organisation adds complexity and expands the attack surface. This means organisations have to begin monitoring these MSPs.

At the same time, the number of entry points and configuration requirements can quickly become overwhelming, making it increasingly difficult to track, manage and control the organisation's Software as a Service (SaaS) landscape.

As a result, FIs are not only investing in third parties to manage the cloud but they are also investing in continuous SaaS discovery and access and management controls to manage these parties. This quickly reduces the perceived ease and cost-effectiveness of using the cloud.

FIs expressed a need to move away from this bolt-on approach to cloud management. They require a new approach that's more cost effective and doesn't expand the attack surface or introduce additional security concerns.

IMPLEMENTING ZERO-TRUST ARCHITECTURE IN THE CLOUD

The cloud allows FIs to reduce their reliance on legacy systems. And because of the abstraction of the cloud, they can bake in security by design principles such as a zero-trust architecture. While many FIs would like to adopt a cloud-first strategy, many companies are reluctant to go all in on public cloud, preferring multi-cloud or hybrid strategies.

This reluctance stems from a lack of trust in the public cloud because FIs are required to give up their sovereignty. In the long term, FIs plan to take a cloud-first approach, but with a hybrid component that puts security first, allowing them to incrementally test configuration and operability before making a full transition.

Before FIs can embark on a zero trust or cloud-first strategy, they have a number of barriers to overcome. Firstly, they will need to improve communications between security teams and developers to make sure that zero trust security standards are understood and implemented correctly.

Secondly, they will need to create a plan for phasing out the use of legacy systems. One attendee mentioned that their organisation is currently trying to implement isolation techniques in the cloud where possible.

However, they've found that pushing forward with security at all costs is not feasible as many critical services are supported by legacy systems in some way. Simply moving these services into the cloud is not possible as the tolerance for downtime is low.

ADDRESSING SECURITY CONFIGURATION IN THE CLOUD

To operate in the cloud, organisations need to configure hardware and software details to make sure they can interoperate and communicate.

Organisations can use virtual machines (VMs) or containers to configure the cloud. A container is an isolated, lightweight silo for running an application on the host operating system. The container is built on top of the host operating system's kernel. In contrast, VMs run a complete operating system, including its own kernel.

Configuration errors in the cloud are common and can have serious consequences. For instance, during the Capital One data breach hackers exploited a misconfigured firewall to gain access to 100 million card details. Attackers can also conduct VM or container escaping attacks where they gain access to the underlying host server, allowing them to move freely around the environment. An organisation's choice between VMs and containers is important for reducing these risks.

Many organisations prefer to use containers as they are lightweight, mobile and can be spun up or retired more quickly. This is of particular use to organisations that are developer-led. But because of the fast-paced, agile nature of containers, configuration errors and escaping attacks are more common than in VMs. Security teams need to respond quickly to developers to ensure that controls are implemented correctly.

Some barriers prevent security teams from communicating their needs to developers. Attendees commented that configuration errors occur because of a lack of best practice standards for containerisation, such as privileged access management.

Whereas escaping attacks occur because organisations don't always have visibility of the underlying fabric. For instance, in the SaaS model the cloud provider can be a fourth party. This means that access to underlying infrastructure is restricted, which prevents organisations from understanding if an escaping attack is possible or if an attack has occurred.

There are tools available that help provide assurance during configuration, such as automated processes for deploying machines and locking them down, firewalls that deny access by default, and tools that scan portfolios and provide alerts if machines have the ability to talk to one another.

But these tools don't directly address the lack of best practice standards and the lack of visibility that FIs are experiencing.

ADOPTING CONSEQUENCE-DRIVEN THREAT MODELLING

The threat landscape has changed during the pandemic because of geopolitical and socioeconomic shifts. At the same time, FIs have changed the way they operate to improve their resilience. For example, they have changed suppliers, increased digital services and implemented remote working.

As a result, FIs are now dealing with new threats and an expanded attack surface.

FIs need to re-examine their threat modelling processes to understand how to secure themselves. Attendees mentioned that they currently use frameworks such as CBEST to create real-world threat scenarios and to integrate threat intelligence into their modelling.

From this, they either implement controls that directly address specific threats or they use a cost-benefit analysis to understand which controls would mitigate the most risk across threats.

Attendees are concerned that current threat modelling approaches don't properly take into account third parties or the wider industry. This means that FIs aren't fully able to map the consequences of a threat. For instance, a small group of Cloud Service Providers (CSPs) dominate the cloud computing industry.

Multiple vendors and other financial institutions may be reliant on the same vendor and even possibly the same data centres. If this CSP experiences downtime in one data centre, the organisation's supply chain, and possibly industry-wide services, are disrupted.

Attendees expressed a need for consequence-driven threat modelling. Here, real-world threat scenarios are mapped in detail from beginning to end, including the short and long-term impacts on the business, supply chains and the wider industry.

While this would be the ideal, FIs don't currently have the capability to map third, fourth and fifth-party dependencies or impacts.

Attendees recognised that there are subtle benefits to this approach. Innovators and vendors who supply FIs with security tools and services would be able to address real needs.

Additionally, as FIs re-evaluate the way they build applications, process data and implement controls, their view of what basic cyber hygiene should look like for the organisation and their third parties will change.

REGULATORS NEED TO UPDATE GUIDELINES AS THREATS AND TECHNOLOGIES EVOLVE

Guidelines and standards such as Cyber Essentials remain important to financial institutions from an insurance, risk, liability and legal perspective. But FIs are concerned that regulators are not updating guidelines quickly enough to keep up the pace at which new threats and technologies are evolving.

While attendees acknowledge that there has been some progress in recent years, they feel that their requirements for reporting, documentation, practices and guidelines would not be met.

Attendees outlined specific needs that regulators need to meet. Firstly, they need regulators to operate in a more dynamic way. They proposed that principle-based regulations or authorised guidance could be used to support organisations, raise standards, and improve awareness when dealing with issues that are complex or evolving quickly.

Secondly, they require greater cohesion and communication between industry leaders, innovators and regulators to address global security threats. Harmonisation between regulators will be particularly important here, as multi-lateral defence will avoid a race to the bottom around auditing, reporting, and requirements.

Lastly, attendees expect that a broad standard for cloud- computing will be developed for the financial services sector. This would clarify the shared responsibility model and specifically address issues like data privacy rules, infrastructure security and inconsistent regulations across regionalised CSPs (European CSPs currently have different recommendations compared to North American CSPs).

There are some developments in this area. Banking authorities are trying to ensure that there's transparency in the cloud. Dutch regulators are trying to get a regional risk hygiene perspective while Tech UK is bringing SMEs together to make sure that organisations understand what's happening in the cloud – especially since many organisations outsource cloud management to Managed Security Service Providers (MSSPs).

LOOKING AHEAD

Over the coming decade, the true digital age will finally arrive. Financial institutions will pursue digital transformation initiatives to increase their agility, which will result in an expanded attack surface because of the use of additional suppliers and a growing dependence on the cloud.

They will remain high-value targets to a range of threat actors, who will increase the sophistication of their attacks and use technology like AI and quantum computing.

In response, financial institutions will need to adopt new threat modelling techniques that account for the changing threat landscape.

They will need to implement zero trust architectures and set new standards of cyber hygiene to better secure their infrastructure and mitigate the risks associated with having a remote workforce, digital customers and an increasing number of suppliers.

Finally, they will need to mature their current cloud and supply chain security practices to better understand their attack surface.

Financial institutions will face many barriers along the way. If regulators are slow to update guidelines and standards, banks may take too long to implement the necessary changes. Meanwhile, limited visibility across the supply chain or cloud and biometric authentication technologies may prevent banks from gaining the level of the security and assurance they need.

THE INNOVATION GAP

Innovators have an opportunity to help financial institutions overcome these barriers and thrive.

For example, they can offer:

- **incentivised supply chain risk management platforms that provide real assurance that suppliers are implementing controls correctly**
- **tools that help banks to properly authenticate the use of biometric identification**
- **education, training and awareness programmes that focus on the risks associated with working from home and deepfake technology**

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre Here
East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS

LORCA BY plexal