DELL Technologies

Security by design – creating a cyber resilient business

The consequences of cyber attacks can be severe – which is why security should be carefully designed into every part of the business rather than just bolted on

By Michael Imeson *Chartered MCSI* and Des O'Connor *senior manager, Cyber Security and AI, Dell Technologies*

'Resilience' is a serious topic of conversation among senior managers and board directors these days. Businesses are weaving operational resilience into the fabric of their strategy to help them manage the rising tide of risks, not least cyber risk, and increase shareholders' confidence in their ability to cope with any eventuality.

Central to the goal of cyber resilience is the concept of 'security by design', whereby security measures are engineered into every part of the business. It is a deliberate approach to cyber risk management that infuses risk thinking into strategic and operational processes. This is in comparison to adding security as a bolt-on to tick a box in reaction to regulatory requirements.

Managing cyber risk is not about piecemeal measures to detect and hopefully prevent ransomware, distributed denial-of-service (DDOS) attacks and other intrusions. It is about having a comprehensive security strategy that ensures the business is resilient to any kind of attack, an objective that governments and public authorities around the world are helping businesses achieve through advice as well as regulation.

Action by government agencies

In the European Union for example, the European Union Agency for Cybersecurity (ENISA) was given far greater powers in 2019 by the EU Cyber Security Act. It is responsible for setting up a cyber security certification framework in the EU for IT products (such as semiconductors), services (such as cloud) and processes (such as information security methods) that member states and businesses will have to adhere to. It has also been given a bigger role in coordinating how EU states respond to cyber incidents.

ENISA teamed up with the European Cybercrime Centre (EC3) in October 2019 to organise a simulated international cyberattack on critical infrastructure to test the EU's Law Enforcement Emergency Response Protocol. The exercise involved 20 cyber crime investigators from private and public sectors working together at EC3's offices in the Hague. The organisers are evaluating the test's findings and will publish a list of actions to improve cyber resilience and the emergency response.

The US is following a similar path. The Cybersecurity and Infrastructure Security Agency (CISA), set up in November 2018, has a broad remit to improve cyber security across public and private sectors. The outsourcing risks facing businesses are one of its areas of focus because no matter how good a firm's security is, its third-party suppliers are often the weakest link. CISA has set up a Supply Chain Risk Management Task Force to help businesses and other organisations address these risks.

Action by financial institutions

Historically, business leaders in the financial sector have delegated operational risk management responsibilities to executives in areas such as fraud prevention, regulatory compliance, data backup and quality assurance. While these are important, the risk horizon has been expanded to include cyber risk and cyber regulation risk.

A good example of this broadening of scope, and the building of security into all operational policies and processes, is the collaboration between US financial services firms on the Sheltered Harbor initiative which protects customer account data if a catastrophic cyber attack or other event causes a firm's systems to fail and data to be compromised. Sheltered Harbor is a not-for-profit subsidiary of the Financial Services – Information Sharing and Analysis Center (FS –ISAC). It comprises banks, asset managers, trade associations, IT providers and other organisations.

Every night, institutions in the initiative back up critical customer account data in a data vault using the Sheltered Harbor standard format. Each institution does the backup itself or uses a service provider. The data vault is separate from the institution's IT infrastructure, including all other backups, and the data is encrypted and unchangeable. If the institution suffers a cyber attack or IT failure, the data is safe and, by activating a 'resiliency plan', can be quickly recovered from the vault to give customers access to their funds. It is something the UK financial sector is looking at with interest.

Action by the capital markets and investment industry

Nearly five years ago the CISI introduced its Managing Cyber Security level 3 award, aimed at capital markets and investment management staff working in information security, anti-fraud, operations, risk management and other areas. The course covers every conceivable aspect of the topic, including the importance of having robust disaster recovery and business continuity plans in place to deal with any type of incident.

> "Recent cyber attacks have shown that it is more important than ever to remain vigilant against cyber adversaries.
>
> – Megan Butler, FCA executive director

The CISI's FinTech Professional Forum organises a cyber security event every year. The next one (date to be confirmed) will be about the operational resilience proposals announced by the Bank of England, Prudential Regulation Authority and Financial Conduct Authority in December 2019 which, at the time of writing, were still out for consultation. The proposals, set out in two consultation papers and a shared policy summary, will require financial firms to improve their operational, including cyber, resilience. Megan Butler, an executive director at the FCA, says recent cyber attacks "have shown that it is more important than ever to remain vigilant against cyber adversaries".

Sector associations are also providing guidance on the problem. The Personal Investment Management and Financial Advice Association (PIMFA) has a Cyber Security Working Group, and its Cyber Resilience Conference 2020 on 29 April will include a presentation by the City of London Police.

The Investment Association (IA) is running a one-day cyber security training programme for existing and aspiring chief information security officers (CISOs) on 21 April. It will examine the role of the CISO in bridging the gap between technology and business at the highest levels, as well as outline best practices for "cyber resilience, including incident management and business continuity".

The IA's third annual Cyber Resilience for Investment Management Forum on 18 May will bring together highly experienced cyber security experts and CISOs from member firms. "The regulators' focus on operational resilience has put cyber and overall resilience in the investment management industry under the microscope," says the association. "Firms are prioritising cyber resilience to ensure they are protected against internal and external threats."

Building security by design

So how do you build security into your corporate strategy so that it becomes part of your business DNA and makes you cyber resilient? There are four key steps to take.

1. Align your risk strategy to wider business resilience parameters including cyber resilience, geopolitical risks and climate change. Ensure that all senior executives – not just the chief risk officer, chief information security officer or other specialist officers – are held accountable for this risk strategy. They should be required to take a long-term approach to risk management.

2. Anticipate new cyber regulation and build it into your security strategy before the compliance deadline. This will ensure greater levels of compliance and make every layer of the organisation more resilient to external threats.

3. Engage the entire organisation and seek input from every team, division and subsidiary into strengthening cyber resilience. By empowering all staff to adopt a security by design approach, your risk strategy will cover all aspects of your business, including third parties and the wider ecosystem. Risks can be assessed and prioritised based on merit and criticality by those who are closest to the activities at risk.

4. Take a strategic approach to assessing your critical data – your 'data crown jewels' – that should be backed up and secured from cyber attack. This can be a complicated task, made more difficult by data managers having different opinions as to what exactly is critical data. Identifying and securing this data also requires support from senior management.

Cyber security and resilience are a major concern for financial services leaders. Security must therefore be engineered into every facet of the business. If it is not, then the likelihood of a serious incident is greatly increased and, as we have seen from countless unfortunate cases, this is an outcome best avoided.