Thinking cyber – at every level of the business

#SWIFT Institute #Market Infrastructures #Cyber-security

With cyber-security concerns an increasing industry priority, Euroclear UK & Ireland CEO John Trundle explains why cyber-threats are a business rather than a technical issue.

Sibos Issues: How do you view the main cyber-threats to businesses in the financial sector today?

John Trundle: We tend to think about the technical threats and of course those threats are real, but the market needs to realise cyber-security is more than having good IT systems. It also concerns a firm's day-to-day 'hygiene.' Good practices include monitoring access to buildings, maintaining password controls and challenging people you don't recognise.

Cyber-risk can involve many kinds of system exploitation that can harm the company, so we make sure our staff are well informed in terms of the threats.

At Euroclear, we do an internal threat assessment in which we work with external specialists to identify and examine different scenarios relevant to our industry. We then categorise them in order, prioritising those scenarios to which we could be most vulnerable.

Sibos Issues: What specific cyber-threats does the industry face on a day-to-day level?

John Trundle: We are well protected against many of the outsider threats, but culturally, it can be difficult to raise the alertness of employees to insider threats. This is because most of our employees are extremely competent professionals, many of whom have been with us for a long time and are highly trustworthy.

But in the absence of any incidents that disrupt the business from an insider perspective, people tend to assume they will never happen and are very trusting. This makes a firm vulnerable if it has a 'bad egg' in the company.

One of the areas we focus on is to make people appropriately aware of security threats from colleagues as well as outsiders, to raise awareness overall. It is easier to imagine the 'bad guy' in another part of the world using high-tech techniques to try to infiltrate the company. It is much harder to imagine a colleague or a visitor committing this type of attack.

There are many potential routes into a company's systems, including the impersonation of business leaders in order to try to initiate a fraudulent transaction. So staff have to be alert, as well as firms being technically resilient to prevent access.

Sibos Issues: How has the task of maintaining cyber-security defences changed in recent years?

John Trundle: We have seen a lot of new potential threats. A firm cannot be complacent, and must remain up to date with best practice in protecting its environment against cyber-threats.

Over the last couple of years, the sophistication around monitoring system traffic has improved significantly. For example, we now have teams that monitor what normal looks like in terms of data exchanges between different parts of the organisation in order to detect unusual patterns.

The timeliness of this procedure has also improved. We can now run separate monitoring systems, 24 hours a day. We have always had operational teams monitoring our systems, but now have separate teams who specifically monitor both external and internal threats from a cyber perspective.

Sibos Issues: Why is it important to see cyber-security as a business issue?

John Trundle: The reason I am speaking at Sibos about cyber-security rather than a head of technology is to show this is a topic that must be owned by the business side as well as the IT side. It has to be shared across the firm.

Business leaders do not need to understand every last detail of the technical threat, but they need to be on top of the broad types of threat that we face and the best ways to try to mitigate, prevent and respond.

It is important to emphasise the business aspect of cyber-security because we run a business process across various high-tech systems, and this process has a number of entry points whose controls are set by the business leaders.

Sibos Issues: What specific measures do you take to train staff in cyber-security practices?

John Trundle: We run a lot of internal training on the risks of sharing information with anyone from outside the company who is trying to access its internal systems.

This kind of training is relevant both to our professional and personal lives, which includes the protection of personal computers. We try to make staff conscious of a wide range of risks, for example by deliberately sending them spam emails and then assessing their responses. I've learnt a great deal personally from this!

Sibos Issues: What should business leaders be doing themselves to address cyber-security issues?

John Trundle: The first priority is to conduct a thorough review, utilising external expertise as necessary; taking into account both technical and business aspects. When we conducted such a review, we identified and analysed scenarios from the perspective of how we might be attacked and the ways in which we might be vulnerable.

The reputational risks of being perceived as not sufficiently strong on cyber-security are significant. Business leaders should recognise this and talk about it openly throughout the business community.

Sibos Issues: What specific measures can business leaders take in the event of a cyber-attack?

John Trundle: There are a number of organisations enabling the sharing of information. These groups are very good at providing advice about potential attacks and informing relevant parties of new forms of attack. This is particularly important in the financial services sector, as firms face similar kinds of threat.

Once under a successful attack, a firm can manage the event as best as possible, but in some respects it's too late if the right measures haven't been taken. All a firm can do then is minimise rather than prevent the damage. We all face the possibility of a successful attack and need to plan for that type of scenario.

Sibos Issues: Are any particular business streams more susceptible to threats than others?

John Trundle: A question that everyone in the financial services industry is asking itself is 'why target me?' The fact is we are all in the firing line as there are so many external threats.

The financial services sector is a natural target because we sit on high values which are readily mobile. Accepting that we are prime targets, firms such as Euroclear need to monitor intelligence constantly to gauge threat levels, but even if there isn't a specific immediate threat, we should recognise there is an ongoing general risk.

The industry can counter cyber-security risks using closed, highly-secure systems accessible to only a small group of known counterparties. But even when the centre of these systems is highly secure, we still need to think about the security of the system as a whole.

There is no way we can stop ourselves from being a target, but we can ensure our defences are varied and effective. ■

TO LEARN MORE …

Business leaders - Think cyber
Wednesday 28 September – 10:15-10:45