Tomorrow's CFO®

Financial Focus white paper - January 2022

'As cyber-crime increases, are we protecting the right things on the risk register?'

Catherine Powell, Managing Consultant - Metapraxis

Tomorrow's CFO Forum Series

This paper has been produced following a round table discussion attended by representatives from industry, accounting firms, accounting bodies and financial journals, and is primarily focussed on the UK market.

Contributors include:

Simon Bittlestone	CEO, Metapraxis
Martin Clements CMG OBE	Senior Advisor to the Chairman & CEO, Credit Suisse Group
Marc Cadwaladr	former Group Financial Controller, Land Securities
John Reeve	former Chairman and Chief Executive, Willis Group
Kelvin Stagg	CFO, PageGroup
John Neill CBE	Chairman & CEO, Unipart Group
Mark Sherwood-Edwards	Founder, Clearview Legal
Christiane Wuillamie OBE	CEO, Pyxis Culture Technologies
Andrew Mercieca	CFO, LifeArc
Lawson Carmichael	Chief Membership & Operating Officer, AICPA
Tessa Drysdale	HR Director, Dogs Trust
Daniele Pedrazzoli	Principal, DPED Consulting

"It's not if an attack is going to happen, it's when it's going to happen."

John Neill CBE – Chairman & CEO, Unipart Group

There is no doubt that cyber-crime and ransomware attacks are on the rise. Businesses are being forced to rapidly adapt to remote working. For many, moving systems and processes online has significantly increased their security vulnerabilities. These lowered defences, and the opportunistic behaviour of hackers, has caused attacks to soar over the last 2 years.

Martin Clements CMG OBE, who has extensive experience in offensive cyber operations, opened the discussion by stating that many attacks are not as sophisticated as we might think, but companies make basic mistakes and get hit.

"First - Don't get hit,
Second - if you do, manage it well."

Either through basic mistakes or simply due to the increased volume of attempted attacks, the likelihood of avoiding an attack is dwindling. According to the 2021 Cyberthreat Defense Report by CyberEdge Group, 86.2% of surveyed organisations had been affected by a successful cyber-attack. Therefore, it is becoming increasingly vital that businesses focus on their ability to "manage it well".

An example referenced by Martin is Norsk Hydro, one of the world's largest aluminium companies, who were the target of a ransomware attack in March 2019 which crippled operations and stalled productions. They decided not to pay the ransom which cost an estimated $70 million in losses.[1] However, they were praised for their transparency and decisive handling of the situation and their stock price actually increased in the wake of the attack due to increased investor confidence in management.

To pay or not to pay

The decision to pay a ransomware demand or not can be painfully difficult. Refusing to pay prolongs the ordeal, further damaging operations, negatively affecting customers and can be catastrophic to a company's reputation. Financially, companies may also be worse off – to date in 2021 the average cost to remediate a ransomware attack has risen to $1.5 million, more than double the average in 2020 ($761,106).[2] [3]

On the other hand, alongside the moral dilemma of paying into the criminal system and incentivising further criminal activity, there is no guarantee that the attackers will release the systems undamaged even if the ransom is paid. There is also the risk that having paid one ransom, the business identifies itself as an attractive target for future attacks.

Planning ahead is critical. Consideration must be given to what is lawful, what aligns with the business values and whether cyber insurance could be used to mitigate costs. An issue that was clear from the discussion is that there is little help from governments or consistent legislation to provide guidance to businesses.

Simulations

A key takeaway from the round table was the necessity for businesses to review and rehearse their approach to an attack long before one occurs. Running regular simulations ensures there is a plan in place and the key personnel know what to expect both of an attack and each other. Many external consultancies offer this service.

The consensus, for those who have been involved in these kinds of simulations, was that groups were much more empowered and effective after the exercises to deal with a real cyber-attack. The simulations highlight how quickly attacks can occur and progress, allowing the group to decide in advance who will take charge of what – for example internal and external communication.

"Plans are nothing, planning is everything, as Eisenhower famously once said."

Mark Sherwood-Edwards – Founder, Clearview Legal

Running these simulations also offers assurance and gives confidence to the wider business that the management are being proactive and that security matters to them. Externally, in the event of a real attack, regulators will ask how well an organisation was prepared for one, so having solid plans and practices in place will also go a long way to minimising future regulator penalties in the wake of an attack.

Digital Age Leadership

Leaders need to take the threat of cyber-crime seriously. They must inform themselves of threats, demonstrate an understanding of digital risk to customers and investors, and exercise preventative measures.

"Cyber-security should be boring, and your job is to keep it that way. If it becomes exciting, you're probably doing something wrong."

Martin Clements CMG OBE – Senior Advisor to the Chairman and CEO, Credit Suisse Group

The forum shared multiple ways businesses should protect themselves. The most important factor is to make sure you have the right people. It sounds simple, but many businesses fail to address both executive and non-executive oversight of cybercrime risk. Other focus areas include the use of independent reviews, instilling a culture of ongoing process improvements, continually testing for security gaps and, the use of simulations.

There are both good and bad examples of business leadership in this area; many of the participants in this discussion have seen both. Ultimately the group's advice was to focus on the "human factor" by making sure the right people were being proactive about cyber-crime, taking steps to improve basic cyber-hygiene and asking the right questions on a continuous basis.

The Risk of Suppliers

An area of risk highlighted by the discussion is third party suppliers. A business can be as cautious as possible within their own operations, but if suppliers and other third parties are not part of the security assessment, there are still huge vulnerabilities.

One incident cited was of an organisation that experienced a ransomware attack against a key supplier. The business itself had prepared thoroughly, with a proactive Head of Information Security, ISO 270001 standards in place, systems reviews and strong data protection. However, they had not focused on their suppliers and unfortunately, despite having received up to date security certificates two months prior, this oversight led to a vulnerability via an old supplier server that affected several parts of the supply chain.

Today that business now has an agreement in place with the supplier to complete regular audits and has put further assessments and protections in place to reduce future risks.

This story also raised a concern from the group that qualifications and certifications can lead to a false sense of security. Not only for third parties but also within companies, certifications or qualifications can provide a sense of comfort when, in reality, they are often used as a tick-box exercise without the detailed thought process to accompany it. The consensus was that the certifications and qualifications can be a good starting point but should be used as a platform to build good practice and data resilience on.

"Organisations need to look at cyber as an enterprise-wide issue, at all processes, IT and suppliers as an ecosystem. To get better, this needs to be about more than just technology."

Christiane Wuillamie OBE – CEO, Pyxis Culture Technologies

Employee Empowerment

The power to defend against cyber-attacks cannot only sit with the board and senior leadership. Employees must be informed and empowered to act when they see something suspicious. This can be instrumental in identifying and lessening the impact of an attack.

One striking example of where this paid off was provided – the company in question was hit by an encryption and ransomware demand on their systems early on a Sunday morning and the team that spotted the attack was able to shut down the systems within 2 minutes, drastically reducing the damage caused. If the team had not had the authority and expertise to do so, an escalation procedure could have cost valuable time and led to an immensely costly recovery process. In this example, the business decided not to pay the ransom. However, even with the quick action to shut down the systems, the recovery efforts took 3 months and cost the organisation millions.

"The most critical thing is early detection. If hackers want to get in, they will, so detection down to minutes and seconds is absolutely vital."

John Reeve – former Chairman & CEO, Willis Group

Collaboration

How can businesses better collaborate against the threat? Hackers often collaborate, working together to organise attacks, yet target organisations seem reluctant to work together.

Cyber-criminals also often attack multiple organisations at once, but businesses don't necessarily work to defend themselves together. This could be due to the fear of exposing a weakness to the competition or the opportunity to take advantage of one.

However, businesses would be in a much stronger position collectively if they joined forces. This could be during an attack, by sharing resources and coordinating defence and recovery efforts, as well as by learning from the experiences of others. This collaboration would lead to much better preparation for, identification of, and response to attacks.

The National Cyber Security Centre in the UK provides expertise and guidance, offers recovery support, and publicises lessons learned.[4] This can be very effective, but the key advice is to encourage people and organisations to talk to each other.

The cost of not investing in cyber-security

The final point of discussion was on the lack of prioritisation and investment in high-quality cyber security. Cyber security is often seen to be neglected or bolted on as an afterthought when it should be a key focus. Ultimately everything and everyone is connected today, so businesses and individuals need to be demanding better quality security.

In the experiences of the discussion group, security needs to be effectively designed from the start, with a focus on quality, an appropriate budget, the right skills hired, and the right people empowered to execute the processes.

"Managing digital risk and improving digital resilience is a tax worth paying, and it is easier to pay if set against the benefits."

Martin Clements CMG OBE – Senior Advisor to the Chairman & CEO, Credit Suisse Group

Investment in cyber-security may in part be limited because the cost of data loss is not immediately apparent. Rarely is the value of a company's data measured reliably and featured on the balance sheet. If the value of data within a business was captured and quantified more effectively it would be easier to justify the large expense required to protect it.

There are many varied financial costs that come from a data breach, from very tangible costs of recovery efforts or regulator fines to the less quantifiable costs like the loss of trust of customers and the damage to reputation. Companies should be seeking to understand the value and the risks of all of these when considering their approach to cyber-security.

Conclusion

It is clear that cyber-crime is an increasing risk for businesses and is not always given the investment and attention it merits. The leadership of an organisation is critical in reducing the threat and damage of an attack, but the biggest key to success is in adequate preparation and getting the basics right.

Ensuring the organisation has the right skills and the right people are empowered to act quickly can go a long way to mitigating the potentially catastrophic harm caused by cyber-crime. Perhaps the most important advice is to consider the true cost of a data breach, if more companies did this the likelihood is that they would be better prepared.

Footnotes

1. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
2. https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
3. https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx
4. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

About the Tomorrow's CFO® Forum

Run in collaboration with the Association of International Certified Professional Accountants (AICPA & CIMA), as part of the Tomorrow's CFO® initiative, these invitation-only roundtables are designed to facilitate engagement amongst a community of senior finance practitioners, and offer an opportunity for finance leaders to share knowledge, experience and expertise directly with their peers.

To address the most pressing issues concerning the future of the finance profession, each Forum event focuses on a specific and challenging question, chosen to stir opinion and provoke debate.

Tomorrow's CFO® Forums are held on a regular basis throughout the year. If you are a senior finance practitioner, and you would like to be a part of future events, then please visit the Tomorrow's CFO® page at metapraxis.com to leave your details and express an interest.

About Metapraxis

Metapraxis enables better decisions through faster and more efficient planning and analysis. Our Empower Technology integrates your financial planning, analysis and reporting activities in a powerful and flexible platform, providing an essential backbone for all your decision-making.

www.metapraxis.com