SOPHOS
Cybersecurity evolved.

8 Steps to Fight Ransomware in the Retail Sector

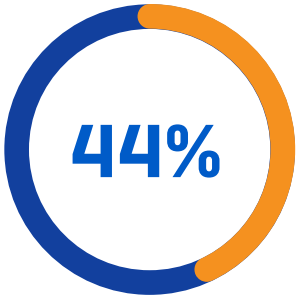
A Sophos Whitepaper. October 2021

Contents

1. The threat to retail

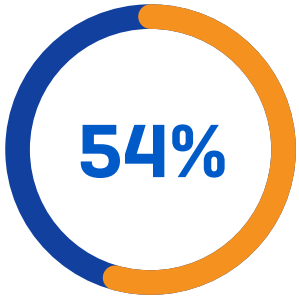
Ransomware is a threat that hangs over all sectors, but some are still more likely to be targeted than others. Sophos research for the global State of Ransomware in Retail 2021 survey found that during 2020 retail was joint top for recorded ransomware attacks along with education. In total, 44% of retail organisations taking part in the survey said they'd been affected by ransomware in the previous year, with a further 34% predicting they'd be targeted in future.

Just over half of those affected had data encrypted during attacks. A total of 32% of retail victims paid an average of £111K to get their data back, but this was only the beginning of a recovery bill that ran to £1.48M per incident when additional costs were tallied. Unfortunately, even those who paid recovered only 67% of their data with only 9% recovering all their data. In a strong indication of how the ransomware modus operandi is evolving, 12% of retail victims said they had zero data encrypted but were still held to ransom using the threat that sensitive data would be made public if they refused to pay.



of retail organizations were hit by ransomware in the last year

The retail sector was hit by ransomware 19% more often than the cross-sector average



of retail organizations said the cybercriminals succeeded in encrypting their data

US$ 147,811

was the average ransom paid by mid-sized retail organizations

US$ 1.97M

was the average bill for rectifying a retail ransomware attack

of retail organizations experienced extortion-style attacks where data was not encrypted but the victim was still held to ransom

Although ransomware is not the only cybersecurity risk the retail sector must cope with, it is clearly one of the most complex and expensive to assess in terms of calculating business risk and response. For CIOs and CISOs, these statistics underscore important conclusions, the first of which won't come as news to anyone in retail: the likelihood of a successful attack at some point is now extremely high. Secondly, the price of a compromise is rising to reach non-trivial sums with those costs growing with every survey.

More optimistically, not all organisations fall prey. Becoming a victim of ransomware is a measurable risk but it is not inevitable that it will lead to disaster. Some organisations seem able to formulate successful strategies to mitigate the risk of attack as well as to recover from the incidents that do occur. The perfect example of this are backup routines, used by 56% of affected retail organisations to recover data without paying a ransom.

CIO strategies

The challenge for CIOs is that as compelling as this analysis sounds, putting it into practice in many organisations is easier said than done. Investing in and testing backup is one necessity, as is the importance of having an incident response plan, including the skills and testing to make that defence more than mere tick box reassurance. But all retail organisations already have backup systems and 91% of respondents who took part in the State of Ransomware in Retail 2021 survey said they had a malware incident response plan in place. The fact that many of these organisations still fall prey to ransomware suggests having a capability and successfully using it are not the same thing.

Coping with modern cyberattacks, including but not limited to ransomware, means being able to make judicious investments when they are required. That, in turn, requires, board approval and that raises the single biggest challenge faced by an CIO: explaining and justifying new investments, which might have to continue for the foreseeable future. That is not a technical problem so much a political and business one, which raises the issue of how technically-minded cybersecurity professionals approach the problem of getting board acceptance of the urgent need to invest.

This is doubly acute when the CIOs find themselves returning to the board year on year with the same request for extra money, possibly following predecessors who made similar demands in the past. This is bound to attract executive scrutiny: didn't we invest a lot of money in cybersecurity last year?

Based on an interview with Diageo CIO, Benedetto Conversano, this guide is an attempt to sketch out some strategies CIOs can follow when interacting with board members on the topic of cybersecurity and the need to make investment in it a priority.

2. Strategies for communicating cybersecurity risk

"Boards have various degrees of understanding of cybersecurity, from direct business experience to what they read from newspapers. That is a big challenge for CIOs and CISOs because you are discussing a very technical subject that requires a lot of expertise with a board that has a very heterogenous understanding of what cybersecurity entails. This often creates a profound communication challenge between the CIO and the board."

Benedetto Conversano, Chief Information Officer, Diageo

As all CIOs discover at some point, talking to company boards about cybersecurity risk and the importance of security investment can be challenging. One barrier is that today's boards comprise business experts whose technical knowledge varies from modest to almost zero. For many board members, this will seem reasonable. Historically, technology has been seen over many decades as something that optimises or accelerates traditional business processes such as forecasting, accounting, inventory, and communication. To the traditionalist, cybersecurity is part of this IT function which, in turn, is only one department in a much larger organisation.

Today, however, the digital element provided by IT has become fundamental to every organisation's wellbeing. Anything that disrupts this evolution automatically threatens its reputation and future financial viability. IT is no longer a mere enabler but in many cases has become the business. Unfortunately, this transformation – and its interaction with cybercrime risk – has happened within a handful of years, faster than many board members have been able to adapt their thinking. CIOs and CISOs find themselves on the front line of the process of re-educating board members about risks that would barely have existed even five years ago.

It is the dramatic increase in risk in a short period that of time has compounded the task of re-education. The conversation CIOs and CISOs might have initiated about cybercrime risks and threats a few years ago is probably very different from the one they might have today. Returning year after year with a slightly different but increasingly alarming message isn't easy when it is combined with a request for additional spending. The inherent unpredictability of cybercrime in which new and more perilous threats emerge suddenly within months or weeks, between spending cycles, only compounds this problem.

Faced with such an uphill task, Conversano's recommendation is to break the job of getting the message over to boards into a series of logical steps which, he stresses, should not be taken as prescriptive.

Step 1: Research board members

"It's becoming more common that board members will have personal experience of a past breach and will understand the destructive potential of cybersecurity."

Benedetto Conversano, Chief Information Officer, Diageo

The first step for any CIO is to analyse the makeup and experience of the board itself. Some of this will be implied by their job role – marketing, sales, finance, CEO roles - but it's worth doing deeper research on their career background and experience, especially the organisations they're worked for and those organisations' history.

Such research is critical because, as the above comment by Conversano underlines, the lived experience of cybersecurity disaster has sadly expanded in recent years. Regardless of the knowledge level implied by a board member's role, if they have seen the consequences of a cybersecurity failure first-hand, they are a potential ally when it comes to making the case for additional expenditure.

Bear in mind that while every board member will have read about attacks from newspaper articles, this does not mean they understand what causes attacks or how they can be avoided. For those without personal experience of a cyberattack, media stories will likely be viewed as interesting but remote. Occasionally, board members will be former CIOs who will be fully aware of the need for a conversation on security and risk, but Conversano cautions that this is unusual.

Step 2: Develop a common language

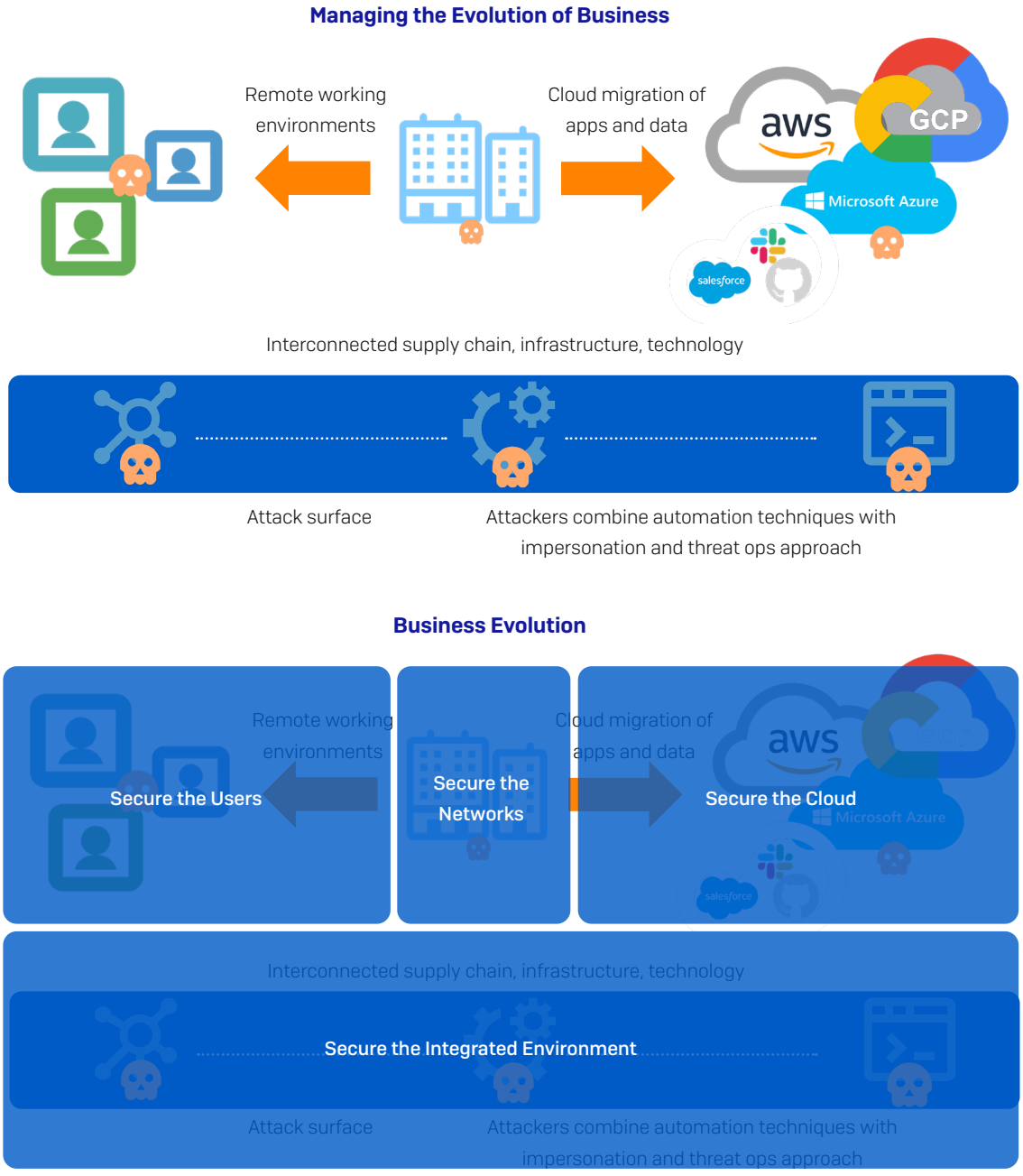
"You have to give the board a pedagogical explanation of how a cybersecurity architecture works in your company. That will create some common ground when you explain what you want to do to strengthen cybersecurity protection."

Benedetto Conversano, Chief Information Officer, Diageo

The next recommendation is one of the easiest to state but the hardest to achieve: find a common language through which to communicate with the board about cybersecurity. What does this mean in concrete terms? What it shouldn't be is overly technical, not simply because this won't be understood but because it doesn't align with the way boards think about risk versus reward.

It is important to describe the job that cybersecurity does without resorting to jargon. The sort of terminology used routinely in IT circles (operating systems, IP addresses, virtual machines, network segmentation, and so on) risks either not being understood out of context or, worse, being misunderstood.

An alternative is to develop a visual representation or model that explains the organisation's cybersecurity architecture as a series of layers which surround certain elements, for example protecting employees, devices, core applications, the network, cloud infrastructure, and sensitive data. This kind of model develops a simple set of reference points that will allow a two-way and more strategic discussion over the long term (see Step 8, Measuring reality).



Step 3: Position cybersecurity as risk management

"Cybersecurity is as significant as every other business risk that the company has."

Benedetto Conversano, Chief Information Officer, Diageo

Cybersecurity is often discussed as being about risk management, a phrase that begs the question of how one characterises this risk and its remediation. The first principle is that cybersecurity risk cannot be eliminated, only mitigated. Technology, additional spending, and better processes cannot remove the possibility of a compromise given the number of variables in play. The board needs to understand this. What matters is to find the best balance between the level of protection for a given level of investment.

When describing this risk, cybersecurity needs to be related to other risks the organisation faces, for example from regulatory action, currency fluctuations, skills shortages, and wider economic and supply chain disruption.

Why has cybersecurity risk risen? Essentially, for three reasons. First, there has been a boom in the cybercrime sector. These organisations are now fully-functioning businesses whose economic model is to prey on others. This development means that the negative consequences arising from this sector are now more destructive than they were several years ago.

Second, most businesses have inadvertently made themselves more vulnerable by making their operation mode digital. Organisations now depend on online sales and digital supply chains and logistics to function. Driven by economic pressures and competition, there is no going back from this state.

Third, critically, as cybercrime has become more destructive, the regulation of industries, including of issues such as privacy, has expanded. Consequently, the financial and reputational risks of a compromise have grown dramatically from it being primarily an internal matter to a very public and even national one. Some boards have found the speed of this change particularly demanding to internalise.

Step 4: Are we okay or not okay?

"The answer to this question is fundamental to educating the board: we are not 100% OK and never will be."

Benedetto Conversano, Chief Information Officer, Diageo

Understandably, the board's top priority in any discussion about cybersecurity is to be given reassurance that the organisation is OK. This is where CIOs need to avoid falling into one of two traps, the first of which is to relieve everyone's stress by telling the board not to worry. This is a mistake because the CIO will end up being attacked if something goes wrong at a later point in time.

Equally, the second trap is to go to the other extreme and tell the board that the organisation is not OK in a way that creates panic. The discussion needs to be sober but realistic. As with any crime sector, the organisation will never be able to compete with the ability of hackers to breach its defences under unusual conditions that are bound to occur occasionally.

In fact, no organisation in the world can stop all cyberattacks. The proof of this is that even some cybersecurity companies themselves have found themselves breached in recent times and those are organisations full of experts that do nothing other than think about how to stop hacking on a 24x7 basis.

Conversano uses the devil takes the hindmost analogy in which to avoid being eaten by a lion, a potential victim need not outrun the animal, only the next person. Although crude, this analogy is a useful way of reminding boards that cybersecurity is now about competitive advantage. Some organisations do it better than others and the ones that take the time to get it right will not only be less likely to fail but more likely to succeed in their wider business aims. Ten years ago, this idea would have been controversial but with every new crippling attack on a large enterprise, the reality of this observation is underlined.

Making cybersecurity a priority isn't simply a way to avoid something bad from happening but a strategy for out-competing peers and rivals with lower standards.

Step 5: Relate investment to KPIs

"You have to align with the board on a specific set of key performance indicators that are linked to the cybersecurity model you want to strengthen and have used to create a common communication framework."

Benedetto Conversano, Chief Information Officer, Diageo

Once the cybersecurity model has been translated into a visual, its effectiveness can be measured using a set of simple cybersecurity key performance indicators (KPIs), which show how progress on specific cybersecurity goals relates to investment. The first task, then, is to decide which KPIs the board will understand as important.

Conversano uses the example of network segmentation, which can be used to contain cybersecurity compromises within certain departments, geographies, or types of vulnerable hardware.

"So, the question becomes, if I want to increase the level of segmentation, how much money do we have to spend, and is that going to be cost effective in terms of reduced risk?" All spending must be explained in this way so that the board can understand the effect spending has had. Equally, too much segmentation makes networks harder and more expensive to manage so the board needs to understand that this is always about balance and is not a magic protection.

Another important cybersecurity KPI might be the number of Windows 7 machines in the organisation. One year, the number might be 2% of the installed base with the KPI of reducing it to 1% the following year, and zero the year after. Ditto, the organisation's resistance to phishing attacks as measured during dedicated exercises that test employee reactions. If the first exercise finds that 10% are susceptible to phishing emails, the KPI should be to reduce this to 5% or 2% a year later.

"Each KPI gives you quantifiable evidence of where you are and the level of protection you have achieved over time. Every investment should be linked to a KPI and its subsequent improvement."

KPI Scorecard

	Objectives	Current	End FY 21 Target	End FY 22 Target	On Target?
Objectives	Reduce % of Windows Machines	7%	5%	2%	Yes
	Reduce % of employees clicking during phishing simulations	15%	10%	8%	No

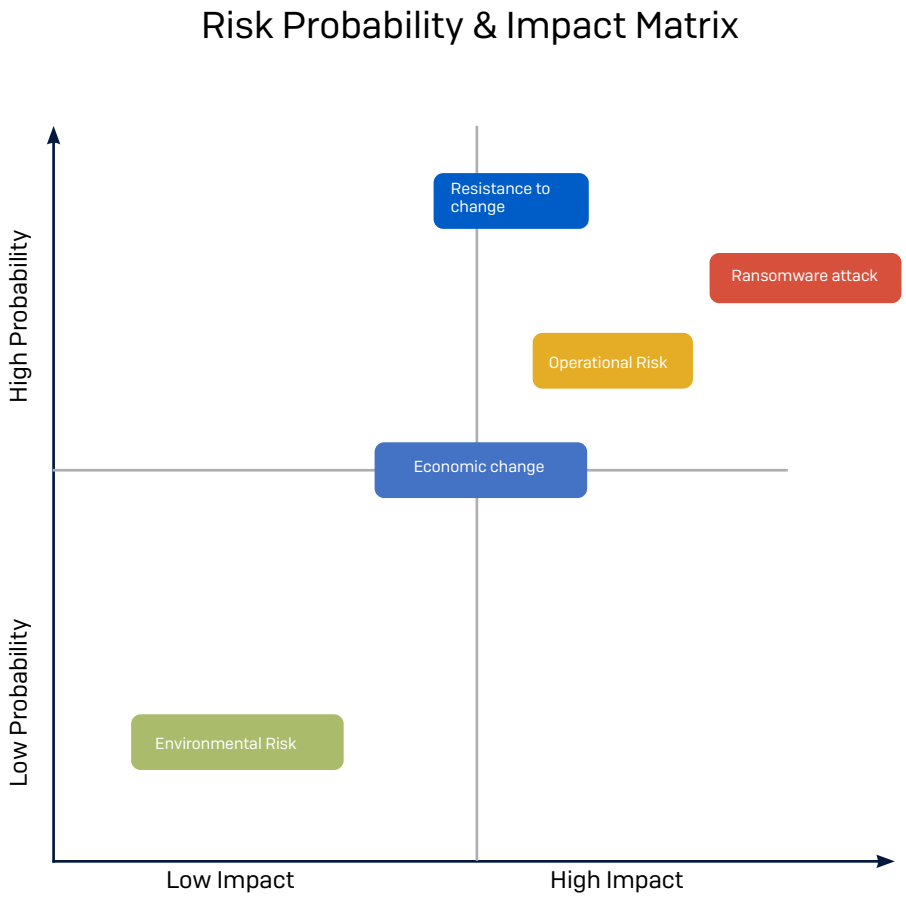
Step 6: Focus on impacts rather than threats

"In today's world, cybersecurity can be characterised as a high impact event with a high likelihood."

Benedetto Conversano, Chief Information Officer, Diageo

Rather than discussing the vague concept of 'threats', it is better to talk to the board about impacts, that is the measurable effect of a compromise or breach. The first of these is the direct disruption to the business in terms of its ability to sell its products, transport them, or to invoice for them. The second effect is the impact on reputation, which might affect the ability to sell products or invoice for them in future. Finally, there are potential regulatory implications which, as with the first two, will have financial implications.

Conversano uses the idea of an impact matrix to explain the effect of each on a scale from low to high on one axis, with the likelihood of each of these from low to high on the other axis. Indeed, identical matrices could be used to describe any risk faced by the business. What marks cybersecurity out from other risks is that within the space of a handful of years it has risen from a medium impact, medium likelihood event to one that is high impact, high likelihood in a way not all board members will fully appreciate.



Step 7: Create and test a ransomware policy in advance

"I always say to a board that it's not a matter of 'if' we will be attacked, but when. What you don't want is to find yourself in a situation where the organisation has been affected by ransomware and there are no company principles in place that say how to behave in those circumstances."

Benedetto Conversano, Chief Information Officer, Diageo

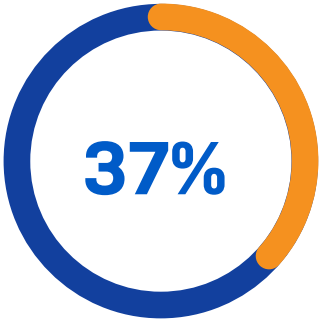
If the board fully absorbs the idea that a successful attack is inevitable at some point, the conversation must move from investment in defence and mitigation to recovery. A critical element of this is to prepare for the eventuality of a compromise in advance and to agree on a strategy for coping with it.

Ransomware is the perfect example. This type of attack is designed to unfold so rapidly it removes the thinking room an organisation might have assumed it had. The ransom demand has been made, the clock is ticking, and the decision to pay or not to pay looms.

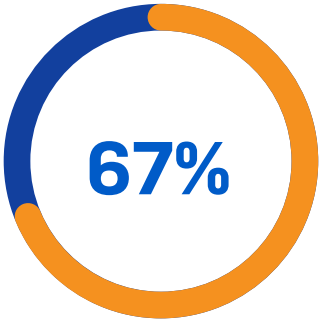
The only way to cope with this scenario is for the CIO and the board to jointly formulate a ransomware policy in advance. Ideally, the robustness of this policy should be tested under simulated conditions to iron out any problems. including a thorough assessment of whether cyber-insurance will be effective to contain financial risks.

Evidence from Sophos suggests that paying ransoms offers, at best, a weak guarantee that all the data encrypted or stolen will be decrypted, returned, or destroyed. According to the Sophos State of Ransomware in Retail report 2021, around a third of global retail victims of ransomware pay up but retrieve an average of only two thirds of their data (see The threat to retail).

A second dimension to this discussion is insurance against the effects of a ransomware or other cyberattack. It is unlikely this will insure the company against all financial and reputational risks, but it can still be a useful mitigation to limit at least limits some of its costs.



Of those whose data encrypted paid the ransom to get their data back



of their data on average those who paid the ransom got back

Step 8: Measuring reality

"You will always get a question from the board asking how well the organisation is doing compared to competitors. Will we outrun the lion?"

Benedetto Conversano, Chief Information Officer, Diageo

The issue of measurement – how you know how well you are doing over time and whether this reflects reality - is the final and perhaps most important element of the way a CIO talks to the board about cybersecurity risk.

Naturally, organisations will adopt high-level governance, regulation and compliance standards (ISO 9001, the NIST Cybersecurity Framework, or the EU GDPR governing data privacy) but these can be quite abstract. A better approach is to refer to progress on operational measurements such as the percentage of devices using encrypted storage, patch management schedules, mitigation of legacy equipment, penetration testing reports, the use of privileged credentials, anti-phishing incident response, and the level of assurance and checking related to supply chain partners.

What matters here is not what each of these means on a technical level but the extent to which the organisation is improving its management of these measurements over time.

One of the ways to achieve this is to conduct an external benchmarking exercise to assess how well the organisation is doing compared to its peers and competitors. This is something boards are guaranteed to ask about and is about proving the adage that when the devil finally takes the hindmost, this organisation won't be the one to get caught. This will give the CIO and board common ground to discuss the organisation's cybersecurity maturity.

3. Conclusion: who is winning?

This basic question is often asked rhetorically during cybersecurity presentations, and there are several possible answers. The simplest and most common is that the cybercriminals are the winners. Collectively, they could be making billions from their crimes and yet their actions remain weakly opposed by the global justice system.

A second, more philosophical answer is that nobody is winning. Cybercrime is just crime, which has always existed and always will exist. It is the entropy in the system everyone else must fight against to keep the system, any system, functioning.

However, there is a third and paradoxical-sounding possibility and that is that a special group of organisations will be the winners in the long term. These organisations – private companies but also public sector organisations and perhaps even governments and entire economies – will be the ones that adapt to cybercrime risk and find a way of coping. They will evolve and adapt while others struggle and wither. Like an economic recession but over much longer timescales, this suggests cybercrime acts as another Darwinian pressure shaping the evolution of business. The organisations who survive will inherit the market or positions of influence from those who don't.

This disturbing possibility is not to say that cybercrime is, therefore, a neutral pressure. It is created by humans and is not a consequence of economic laws that are not well understood or an act of nature nobody could predicts. It is never inevitable. The risk is that it will damage many good organisations doing good work simply because their IT department, CIO and board members were unable to adapt quickly enough to the danger it poses.

It is for this reason that CIOs and boards should invest time and money thinking through the implications of cybersecurity risk before it is too late. History suggests that as incidents grow more serious, governments will intervene, indeed this is already happening with increasing regularity. But the risk to an individual organisation will always be the responsibility of its management. The first job of a forward-looking CIO is to make sure these individuals are well enough informed to act.

4. Further reading and resources

The State of Ransomware 2021
https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx

Four Key Tips from Incident Response Experts
https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-four-key-tips-from-incident-response-experts.pdf

Managed Detection and Response Buyer's Guide
https://news.sophos.com/en-us/2020/09/28/report-managed-detection-and-response-mdr-buyers-guide/

Incident Response Guide
https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/incident-response-guide.aspx

Cybersecurity: The Human Challenge
https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-cybersecurity-the-human-challenge-wp.pdf

2021-09-27-WP(MP)

SOPHOS