censornet.

The real cost of cyber crime.

The CEO guide to cyber security

Ed Macnair
CEO, Censornet

CEOs need to join the fight against record-breaking attacks

CEO's are stepping up

As the modern cyber threat landscape evolves at pace, so too must the role of modern-day CEOs in protecting their organisations.

With the rise of digital crime, insider threats and sophisticated tactics employed by international criminal networks, no company is immune.

As CEOs, we need to take a proactive role in preparing our organisations to mitigate the risk of cyber-crime, whilst protecting our finances against potential losses.

The financial consequences can be severe and, critically, unexpected. Consider GDPR regulatory fines, reputational risk, share price impacts, the cash flow impacts from ransoms, and higher insurance costs. And that is before you take into account system downtime (sometimes for months) and loss of business efficacy.

Hackers are shifting from "big-game" to mid-sized targets

A third of businesses are suffering a breach or attack every week, and with this, we are seeing record-breaking ransom demands. REvil, notoriously, asked for $70 million to end its attack on Kaseya. It's not just high-profile targets that are under attack

In 2022, the UK's National Cyber Security Centre (NCSC) in partnership with the Federal Bureau of Investigation (FBI), National Security Agency (NSA) and Australian Cyber Security Centre, advised that hackers were shifting from "big-game" to mid-sized targets.

Cyber security has become a team sport – and the CEO's role in is pivotal.

Cyber security is no longer the sole remit of security teams. Close collaboration between IT experts and CEOs is vital to ensure maximum protection.

Without this, CEOs are left out of the loop on cyber issues which threaten the business with significant financial consequences.

It's essential we prioritise cyber security investments and start to build the knowledge and resources necessary to combat these threats head-on.

Technology advancements have lowered the bar for launching an attack and increasingly powerful computers allow for rapid execution.

It has never been more important to stay ahead.

Section 1:

The real and present danger

The threat landscape

As many as two in three (65%) mid-market organisations have suffered an outage, with half (33%) seeing systems knocked offline for more than a day. These incidents were driven in part by the unwitting insider threat: 17% of respondents reported serious attacks after employees opened suspicious or malicious emails, with that number rising to 28% for businesses turning over more than £51million.

Organisations don't just stand to lose time and customers:

> **30% suffered a data loss because of a cyber-attack in 2021, with that figure rising to 36% for smaller businesses turning over between £1- £5 million a year.**

The full extent of stolen intellectual property is not always immediately apparent. It's not just the sleepless nights. Supply chains are being interrupted. In February 2022, a supplier of components to Toyota was hit by a suspected cyber attack. It forced the world's largest car-maker to close all of its factories in Japan for the entire day. The net result, it had to halt production on 13,000 vehicles.

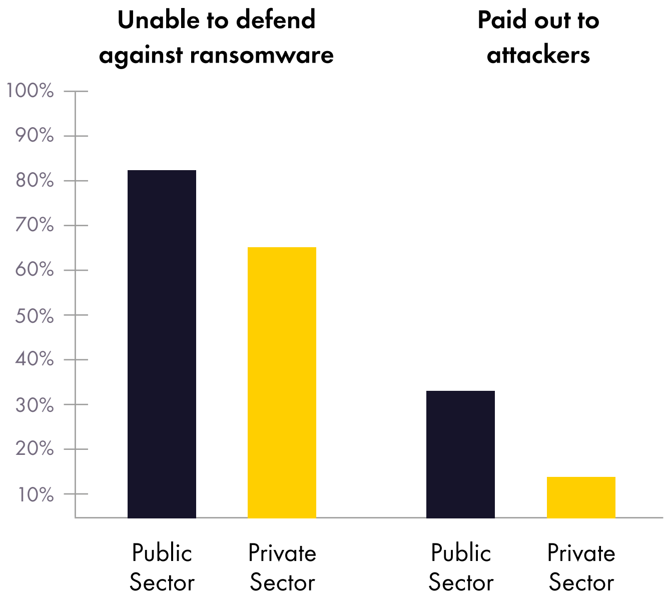
One in five pay their ransom

A closer look at ransomware illustrates the potential severity of a security breach. More than two thirds (69%) of mid-size companies didn't feel able to protect themselves against ransomware, and with good reason.

Over the year, one in five (21%) suffered a ransomware attack and subsequently paid the ransom. The average pay-out was £144,000, with 7% of those handing over in excess of £500,000.

Public sector organisations were worse affected than their private sector counterparts. A huge 83% reported they felt unable to defend against ransomware, compared to only 65% of private sector organisations. And a third (34%) eventually paid out to attackers, compared to 14% in the private sector.

The picture is all too clear: despite a wide range of point solutions on the market, organisations are still paying the price for inadequate defence, particularly in the hard-pressed public sector. When budgets and staff time are squeezed, a more intelligent approach is needed to tip the scales.



Ignorance is not bliss

Research shows CEOs are overwhelmingly confident in their companies' abilities to detect and respond to cyber incidents. Recent headlines, however, paint a different picture. Even for a company with sizable resources. CEO's should no longer claim ignorance to the potential threats.

Northern Power Grid

An estimated **£200 million** was lost when hackers managed to gain access to the National Grid's systems and take down power lines across the region. The attack was so severe that it took days for full power to be restored, leaving thousands of businesses and households without electricity for an extended period of time.

The Bank Heist

A sophisticated cybercriminal group managed to infiltrate several major banks in London and steal millions of pounds from customer accounts. Although the precise amount taken has never been revealed, it is believed to be at least £150 million and could even be as high as **£250 million**.

The Home Office

This attack saw hackers break into the internal systems of the Home Office and steal confidential data related to more than two hundred thousand people living in the UK, causing massive disruption and untold costs to repair the damage. Estimates place this cyber-attack's cost at more than **£100 million**.

Heathrow Airport

In this incident, attackers were able to gain access to security systems at Heathrow Airport and cause major chaos for passengers trying to pass through immigration checkpoints or board flights. Airlines had to cancel hundreds of flights, resulting in an estimated financial impact on them alone reaching around **£70 million**.

NHS

An unknown hacker group succeeded in breaching NHS systems across England and Wales, causing system outages that resulted in hospital appointments being cancelled or delayed and medical records being inaccessible for days at a time – costing an estimated combined total of **£50 million** between lost productivity and emergency repairs conducted by IT specialists working around the clock.

Section 2:

The real cost of cyber crime

censornet.

Impacted cash flow

The losses resulting from a successful breach can have a detrimental impact on cash flow. With direct losses, and lost revenue from downtime, it can make business-as-usual expenses a struggle.

Some companies have defaulted on credit card or loan payments following a breach, further impacting their credit rating and forcing a drastic cut in costs.

Business disruption

One of the most significant costs that must be factored into cyber-crime is business disruption. This is also among the hardest to quantify in advance, as each case of cyber-crime varies in impact and intensity. Costs can include:

1. Rebuilding operational capabilities, such as repairs to computers or equipment

2. Inability to supply goods or services to customers, resulting in less revenue and potential market share losses

CEO's need to work with security leaders to minimise the disruption and make sure everything is done to prevent it in the first place.

Reputational damage

A successful cyber-breach can have long-lasting effects on the brand and its reputation. It may be a sign to customers, suppliers, and other commercial partners that the organisation is insecure. This can lead to questions around whether governance, risk management and information security controls can be fully trusted.

As CEOs work to safeguard an organisation's brand and financial interests, cyber-crime, and the potential reputational damage, poses a uniquely serious threat.

Working collaboratively with experienced cyber security specialists is essential for identifying risks that may otherwise be overlooked. It's also important to develop precautionary measures and effective strategies in defence of any potential malicious activity.

Cyber-attack makes US$350million vanish.

Verizon was set to acquire Yahoo when Yahoo suffered a series of cyber-breaches. As high-profile attacks, they negatively impacted its stock price by 3%. Verizon subsequently declared the breaches to be a "material adverse event" under the Stock Purchase Agreement, and the purchase price was reduced by 7.25%, or US$350 million.[1]

[1] 6 Ways To Protect M&A Deals From Ransomware In 2022, Baker Botts

Impact to credit rating and valuation

Cyber-criminals are exploiting stolen identities for their own gain, applying for loans and credit cards in the victim's name – impacting an organisation's hard-earned reputation and preventing them from accessing much needed financing down the track.

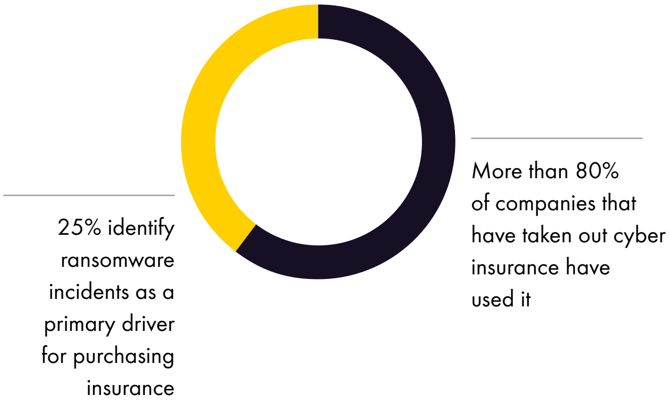
A drop in an organisations credit rating could lead to:

- Higher interest rates when raising debt and
- Doubts about the capacity of senior management among investors and shareholders

Both of these could have a big impact on the company's valuation.

It's vital CEO's recognize the potential impacts of cyber-crime - from credit rating deterioration to restricted access to funding. Partnering with cyber security professionals is paramount in protecting your organisation and avoiding financial losses associated with malicious activity.

The value of cyber insurance



Increased insurance premiums

The decision on whether, or how much, cyber insurance cover to buy is a tough one, even with the rising profile of ransomware attacks. With soaring premium costs making up for "under-priced" cover in 2018-19, it can be an expensive outlay. Some organisations are opting to buy less insurance, or even none at all.

For those that do decide to cover the potential fall out of a cyber breach, the past has consequences. Recent research indicates that some insurers are imposing a 200% premium increase on organisations that have been targeted in cyber-crime.

The potential repercussions for going without insurance are serious, so even with the cost implications, many organisations have no choice. The alternative could be an inability to continue operations.

The role of the modern CEO is no longer limited to financial management. Increasingly, they must also focus on cyber security and ensuring their organisation is well protected against the growing threat of cyber-crime. By working with risk and cyber security experts, CEOs can develop comprehensive strategies to protect their organisation's financial assets.

Section 3:

CEO plan of action

censornet.

5 steps to success

The CEO plays a crucial part in ensuring that cyber security investments match not only the potential risks, but mirrors the value and importance of the company's infrastructure, from financial systems to operational technology networks.

Armed with an awareness of the evolving threat landscape, and the potential financial impacts, how else can CEOs protect their organisation against the impact of cyber-attacks?

Step 1: Quantify the risk

You've read about some extreme attacks where millions have been lost. But what does a breach actually mean to your organisation? Hopefully "The real cost of cyber crime" section will start to paint a picture. Start building scenarios that apply directly to your business, like 'what would be the cost of your business being unable to operate for a day, week or month'?

Step 2: Invest in cyber

Cyber security is an investment that needs to be assigned budget in order to be successful. Decide how much to invest by balancing the desired level of protection and the cost it takes to achieve that outcome.

> **Board and executive mandates for cyber security that lack funding are unrealistic, but security expectations are still being set**[2]

It's important to translate and balance the cost of protection with informed acceptance of the cyber security risks. This is a team exercise, and needs to be an open conversation with your security team.

[2] Measure the Real Cost of Cybersecurity Protection, Gartner, March 2022

5 steps to success

Step 3: Establish board-level security oversight

It's up to the CEO to ensure financial stability and a successful cyber-attack is a big threat to that. But you aren't responsible alone.

Advocating for board-level security oversight promotes board responsibility for cyber security. One consolidated platform that enables custom-made reports means that this isn't an onerous task, but still enables the board to track risk and have insight. It can also make sure your investment is on track!

> 88% of boards now see cybersecurity more as a business risk than a technology risk.[3]

Step 4: Tick the insurance boxes

Want to get cyber security insurance? Requirements vary from insurer to insurer, so it is important to understand the specifics for individual insurers. However, generally speaking, most insurers require that organisations have robust IT security protocols in place and are following best practices.

One of those requirements is security awareness training. Organisations are already seeing claims refused as they are unable to prove any employee training or testing.[4] Insurers know security awareness training is a powerful tool against cyber-criminals, so make sure you have it.

Step 5: Review who needs access to what

CEOs have a responsibility to safeguard their organisation's financial assets. That includes making sure the wrong people don't have access. Adopting appropriate internal controls that restrict the level of information individuals have access to helps mitigate the potential risk of a malicious insider.

This requires tight coordination with your IT team. You need to decide who has access to what, whilst IT ensures that it's reflected in their identity solution (typically **Identity-as-a-Service**, or IDaaS).

[3] https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk
[4] https://www.professionalsecurity.co.uk/news/interviews/cyber-insurance-bottom-line/

Section 4:

How we can help

censornet

Future-proofing your investment

At Censornet, we are revolutionizing the way mid-size businesses manage their security. Our fully integrated platform drastically cuts costs and implementation time so you can get back to focusing on your business's success. Our award-winning UK technical support team is always available when needed – so you can make the move to hassle free cyber security that comes complete with peace of mind.

Reduce your risk with total protection

For millions of users globally, Censornet is already working smarter, faster, and safer than is humanly possible. We verify and assess risk continuously – every person, every cloud, no exceptions. Which means you know that wherever the attack comes from, you are protected.

Our cyber security platform integrates attack intel across email, web, cloud apps and identity to ensure cyber defences react at lightning speed. All your defences, covered.

> **By 2025, nearly half of cybersecurity leaders will change jobs, 25% for different roles entirely due stress[5]**

Censornet take the stress out of total protection. With all your cyber security tools in one place, your security team avoids alert fatigue, whilst you avoid the costs of churn. Total protection, minimal disruption.

Rapid time to value

Censornet can be deployed in a matter of minutes, offering an untouchable time to value. You can have unparalleled protection in a matter of minutes.

We share advanced threat intel across email, web and cloud applications, synthesising a billion threats a day. Our autonomous security engine (ASE) is the brains behind the platform, working at lightning speed, so your IT team can focus on delivering strategic value instead of processing alerts.

Complying with regulations

Not only does our Security Awareness Training make sure you hit insurance requirements, our Data Loss Prevention tool ensures you align with CCPA and GDPR requirements. With complete visibility and control over your data, you can prevent insider threats, negligence or data misuse that could result in fines.

[5] Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, Gartner, January 2023

Find out the cost of Total Protection

Call +44 (0) 845 230 9590 or sales@censornet.com

FEVER-TREE

kpn

LOTUS

covea Insurance

THATCHERS EST. 1904 THE FAMILY CIDER MAKERS

National Portrait Gallery

sanne

NSPCC

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection.

Its Autonomous Integrated Cloud Security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed. For its millions of users globally, its AI-driven, autonomous solution is smarter, faster, and safer than is humanly possible.

Censornet was named Technology Provider of the Year at the British Business Awards 2022. Supported by an award-winning team of customer support specialists, it's leading the way with autonomous integrated security.

Censornet's clients include Macmillian Cancer Support, Fever Tree, Lotus Cars, Parnassia Group, Mizuno, Radius Payments, Newlife Disabled Children's Charity, National Portrait Gallery, Hallmark Hotels and Thatchers Cider.

For more information, please visit www.censornet.com.