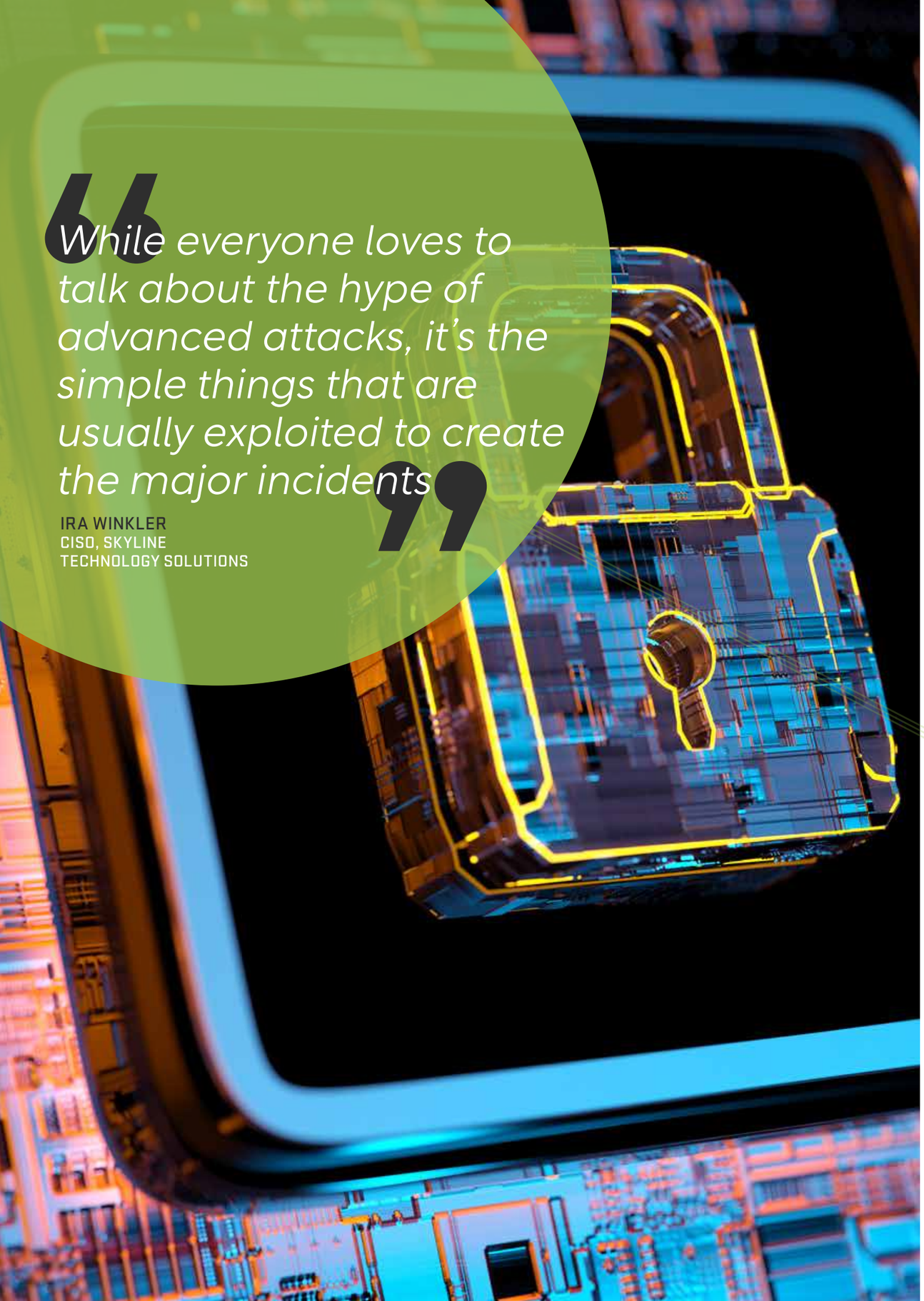
Cyber. WHITE PAPERS

CYBERSECURITY REPORT

Taking Cybersecurity Seriously – How to Get your CEO to Listen Before it's Too Late



While everyone loves to talk about the hype of advanced attacks, it's the simple things that are usually exploited to create the major incidents

IRA WINKLER
CISO, SKYLINE
TECHNOLOGY SOLUTIONS

The biggest cyber security threat to your organisation could be you

Cybersecurity is a major source of anxiety to CEOs, but they still aren't spending on security. Cyber Magazine discusses cyber urgency and complacency

Cybersecurity has fast become a major source of anxiety to businesses worldwide and is now second only to the chaos caused by the pandemic.

That's according to the most recent PwC Global CEO Survey, in which nearly half of CEOs cited cyber as the biggest anxiety in 2021, up from just 33% last year. And among CEOs in North America and Western Europe, it is the top business threat, and therefore the number-one priority for CEOs in North America (69%), Western Europe (44%), the Middle East (41%) and Asia (40%).

And there's good reason for such concern, given the increase in high-visibility cyberattacks that have occurred since the onset of the pandemic, including 2020's most significant – SolarWinds, with hacking of the US IT firm leaving its clients including the US government and Microsoft vulnerable for nine months.

There were many others though in 2020. In March, a major security breach with Marriott International led to the data of more than 5.2 million guests being compromised. In May, healthcare insurance giant Magellan suffered a ransomware attack with up to 365,000 patients impacted. And in July, someone took control of 130 high-profile Twitter accounts (Apple, Elon Musk, Barack Obama) and conned people into sending Bitcoin to an account.

Even as this is being written, "Acer, ironically a tech company, has just been hit by ransomware with the criminals demanding US$50 million", Ira Winkler, CISO of Skyline Technology Solutions, and one of the world's most influential security professionals, tells me.

300%

The increase in reported cybercrimes since the onset of the pandemic, according to the FBI

Cyberattacks happen all the time, and more frequently, and they cause tremendous damage, says Winkler, pointing to the Wannacry virus where organisations around the world suffered crippling outages. Many incidents have been serious enough to lead "to the firing of CEOs", he adds.

And while organisations "which are completely IT-based, like banks, have more dependence on cybersecurity", all types and sizes of organisations can be at risk. "If you're a small business and you cannot service your clients without computers, which these days includes everyone from restaurants to retail stores, you need to be concerned," warns Winkler.

The statistics are scarier still. Since the onset of the pandemic, the FBI has reported that the number of complaints about cyberattacks to its Cyber Division is up as many as 4,000 a day, a 400% increase since the COVID-19 outbreak; Interpol is seeing an "alarming rate of cyberattacks aimed at major corporations, governments, and critical infrastructure"; and according to VMware Carbon Black's latest Modern Bank Heists report, there has been a 118% surge in cyberattacks against banks since 2020.

"Most CISOs spend their time touting the importance of what it is they do, and the reality is that most advice offered by CISOs falls on deaf ears until there is actually a breach"

JEAN-MICHEL AZZOPARDI
CEO, KRALANX CYBER SECURITY

It's the sort of numbers that keep banking CEOs awake at night. Like Uday Kotak, CEO of India-based Kotak Mahindra Bank, who cites cybersecurity as the company's greatest business threat. Having "witnessed increased fraud in the banking system" during the pandemic, Kotak explains that it is the threat of a cyberattack and "the thought of losing my customers' money to theft that keeps me up at night".

Because as Kotak explains, "while COVID has brought about a significant increase in digital adoption and transactions, it has also increased the risk associated with digital".

And with the shift to remote/hybrid working, the risks have been greater still, with many remote workers using insecure data transmission channels to transmit organisational data and organisations lacking in effective enterprise-grade firewalls, antivirus solutions and network security solutions.

Kralanx Cyber Security CEO, Jean-Michel Azzopardi, explains that "information security has broached the frontline" due to the majority of employees now working remotely and this has therefore heavily increased "an enterprise's risk and reliability on information security as a whole".

In her first speech since taking the helm of the UK cybersecurity agency, the National Cyber Security Centre (NCSC) in March 2021, CEO Lindy Cameron warned against company complacency, saying that as "our reliance on technology grows, it sadly also presents opportunities for those who want to do us harm online".

JEAN-MICHEL AZZOPARDI

TITLE: **FOUNDER AND CEO**

COMPANY: **KRALANX CYBER SECURITY**

Founder of Kralanx, a one-stop-shop for advanced cyber security services and consulting located in Malta, Azzopardi has worked with IBM, SAP and Acunetix and has negotiated cyber security deals with companies and governments across Asia including Apple, Huawei and some of the largest Fortune 500 companies worldwide. Having been involved in a number of start-ups, he prides himself in striking a balance between corporate standards and SME efficiency.

IRA WINKLER

TITLE: **CHIEF INFORMATION SECURITY OFFICER**

COMPANY: **SKYLINE TECHNOLOGY SOLUTIONS AND AUTHOR OF YOU CAN STOP STUPID**

Dubbed a 'Modern Day James Bond' by the media, a title he earned by performing espionage simulations where he physical and technically 'broke into' some of the largest companies in the world, investigating crimes against them, and telling them how to cost effectively protect their information and computer infrastructure, Winkler is considered one of the world's most influential security professionals. Starting out at the National Security Agency, Winkler has since designed and implemented support security awareness programs at organisations of all sizes, industry-wide and worldwide.

BUSINESSES NOT TAKING CYBERSECURITY SERIOUSLY

And while our reliance on digital has become much greater, and companies are forging ahead with speedy digital transformations, according to Cameron, cybersecurity is still not taken as seriously as it should be.

And PwC's research backs this up. While nearly half of CEOs are planning increases of 10% or more in their long-term investment in digital transformation, little is being put into cybersecurity technology. So, despite the level of concerns CEOs registered about cyberattacks, just under half of

those planning for heightened digital investment are also planning to boost their spending on cybersecurity and data privacy by 10% or more.

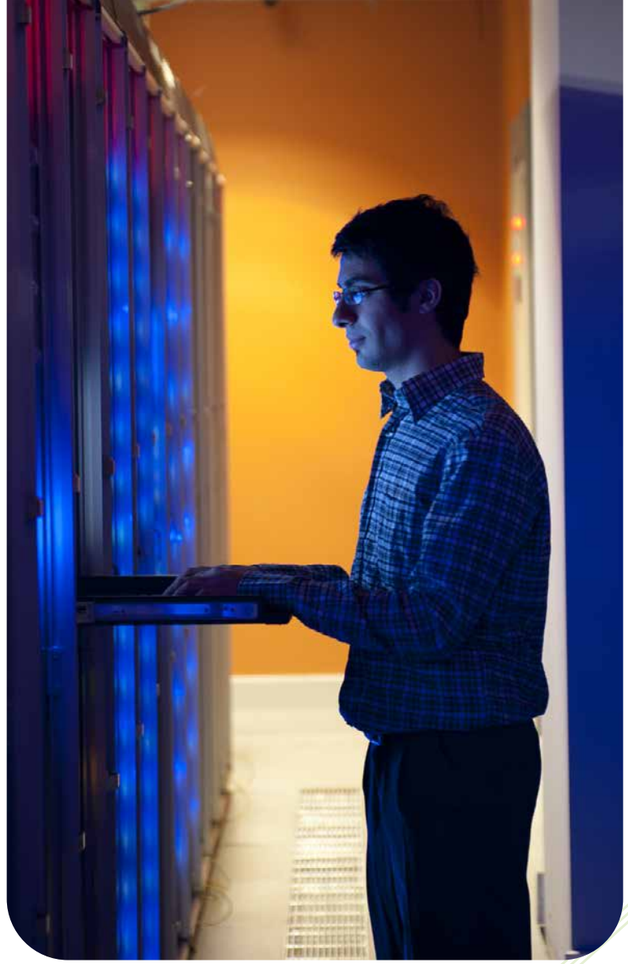
This is not a surprise for Azzopardi, who says that cyber security generally falls quite low on most businesses' priority list due to the fact that there's "no quantifiable value generation from direct investment". And despite the very real urgency, that priority is lower still now due to competing business priorities. "Unfortunately, with many companies cannibalising marketing budgets in order to retain employees, InfoSec has taken a back seat for the most part."

Winkler says he is currently seeing businesses tactically implement security. "They are doing what is obviously required, such as work from home security, but for many companies, they need a strategic rearchitecting of their security, which just isn't happening as much."

Cybersecurity, says Cameron, should be viewed with the same importance to CEOs as finance and legal and "our CEOs should be as close to their CISO as their finance director and general counsel".

Though the stats suggest this simply isn't happening. In the financial sector,

"80% of organisations tell us they have a hard time finding and hiring security professionals"



for example, the majority (75%) of CISOs still report to the CIO rather than the CEO, according to VMWare's Bank Heist report.

Azzopardi agrees, telling Business Chief that while the CISO has certainly become more important than it was previously, it's still not as important as it should be. "Most CISOs spend their time touting the importance of what it is they do, and the reality is that most advice offered by CISOs falls on deaf ears until there is actually a breach. They are the most under-appreciated, and probably the most stressed of the C-suite."

That's assuming of course an organisation can find a CISO. According to Gartner's Research VP Peter Firstbrook, "80% of organisations tell us they have a hard time finding and hiring security professionals, and 71% say it's impacting their ability to deliver security projects within their organisations".

MOST COMMON MISTAKES BUSINESSES MAKE

Not prioritising the CISO role is just one of many mistakes that businesses are making today. According to Winkler, businesses generally don't focus enough on the basics and often focus too much on the obvious when what is actually needed is for firms

"The reality is that the basics matter, we call it cyber hygiene"

"to focus on the underlying architecture".

He points not to a specific cyberattack, like ransomware or phishing, as major threats to businesses in the security landscape, but "enterprise ignorance", along with a company's lack of applying basic security protection. And this, Winkler explains, can lead to big incidents.

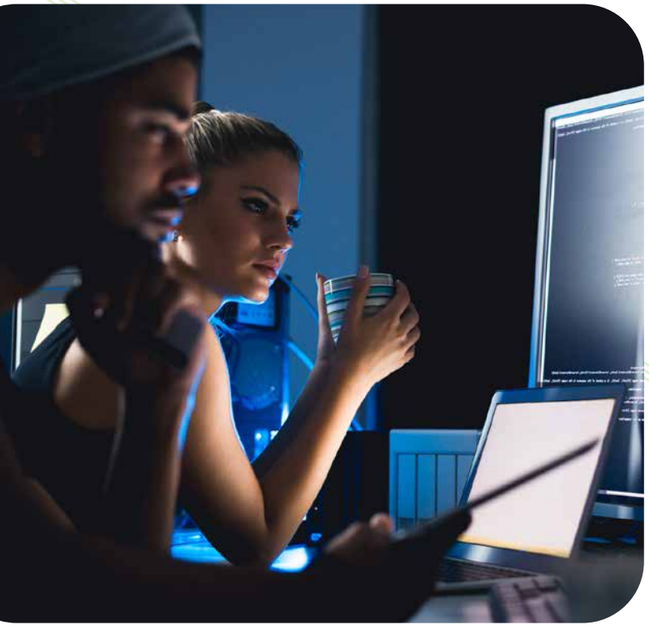
"The reality is that the basics matter, we call it cyber hygiene, so while everyone loves to talk about the hype of advanced attacks, it's the simple things that are usually exploited to create the major incidents. Small businesses are dealing more with end user related issues and have to work on PC security and good passwords, while large companies have to worry about infrastructure concerns."

FROM RANSOMWARE TO DOXWARE

Ransomware attacks, where cybercriminals hold your computer data or network hostage until a ransom is paid, is a serious and growing threat for businesses, both in scale and severity, and isn't just about fraud and theft of money or data, but also "the loss of key services and unenviable choices for unprepared businesses", says Lindy Cameron, CEO of NCSC. And ransomware has upped its game during the pandemic, with attacks up 800%, according to cybersecurity firm MonsterCloud, with founder Zohar Pinhasi suggesting that criminals have now converted ransomware to something called doxware. "If you're not going to pay us, we will sell your data and, in addition to that, notify your customers that you were hacked and that their data was compromised," says Pinhasi. "This is a game-changer since the coronavirus started – we've seen it in the past, but not to this degree."

According to Azzopardi, one of the key mistakes that businesses make is believing that a hack can be detected instantly. The reality is that most companies take on average of six months to detect a data breach, even a major one, as the SolarWinds incident proved. Information such as passwords, credit card details and social security numbers may already be compromised by the time a company is notified.

Azzopardi also explains how businesses, big and small, simply don't



attribute enough importance to the human element. That's despite the fact that 95% of cybersecurity breaches are caused by human error.

"The main point of attack is, and will probably always be, the human element. It's way easier to fool a human than it is to brute force login credentials," explains Azzopardi. "The main issue with phishing is that it's almost impossible to use technology in order to prevent it, instead security awareness training is perhaps our best tool and since we rely on humans to execute such a task, we must assume a significant rate of failure. It is our imperfection after all that makes us human."

3 CYBERSECURITY TRENDS 2021

These techniques, tools and approaches were revealed by analysts at Gartner's Security & Risk Management Summit APAC in March. The summit is further planned globally: London and Florida, in September, and Tokyo in October.

Breach and Attack Simulation
Breach and Attack Simulation (BAS) tools are emerging to provide continuous defensive posture assessments. When CISOs include BAS as a part of their regular security assessments, they can help their teams identify gaps in their security posture more effectively and prioritise security initiatives more efficiently.

Privacy-Enhancing Computation
These techniques protect data while it's being used, rather than while it's at rest or in motion, enabling secure data processing, sharing, cross-border transfers and analytics, even in untrusted environments. Implantations of this are on the rise in fraud analysis, intelligence, data sharing, financial services, pharma and healthcare, and Gartner predicts that by 2025, 50% of large organisations will adopt privacy-enhancing computation for processing data.

Cybersecurity Mesh
This is a modern security approach that consists of deploying controls where they are most needed. Rather than every security tool running in a silo, a cybersecurity mesh enables tools to interoperate by providing foundational security services and centralised policy management and orchestration. With many IT assets now outside traditional enterprise perimeters, a mesh architecture allows firms to extend security controls to distributed assets.

THREATS FACING FINANCIAL INSTITUTIONS IN 2021

According to VMWare's fourth annual Modern Bank Heists report (2021), while the financial services sector is probably one of the most secure, they are dealing with the "most sophisticated cybercrime cartels", says VMware's Head of Cybersecurity Strategy Tom Kellerman. Here are some of the increased risks for banks in the past year.

- **Time stamp manipulation** Criminals now know how to evade detection by manipulating time stamps, so financial institutions need to pay greater attention to securing the integrity of these stamps to ensure this method isn't used to alter the value of capital or trades.
- **Island hopping** This increased 13% (excluding SolarWinds) in 2020 and happens when a hacker attacks an organisation within the large bank's information supply chain and uses a third-party to 'island hop' onto the bank's network. They are not limited to supply-chain vendors or tech firms and once they are inside your infrastructure, will use that to get into your customers and partners' systems too.
- **Targeting Market Strategies** Increase in attacks that target a bank's non-public information and market strategies, suggesting says Kellerman, that cybercrime cartels have become more knowledgeable about

So, what should businesses prioritise in 2021 and beyond? Azzopardi points to the basics such as antivirus, antimalware, password managers and revoking of admin rights as organisational musts. "Throw in mandatory VPN access, regular training and exercises such as BCP testing and your organisation would already be much better prepared than most," he says.

He also says that API security is right up there with companies forced to make certain APIs public. As such, a priority for security teams is to "design a robust and effective API testing strategy that doesn't impede development too much while balancing security".

Finally, he predicts that ransomware will continue to rise, and that cryptojacking will explode. "This is basically the process of creating a bot-net which unknowingly mines crypto for a single wallet. This can be delivered via phishing quite effectively and you will never know it's even there."

$170.4 billion (US)
The forecasted size of the global information security market by 2022, according to Gartner

Cyber. WHITE PAPERS

WRITTEN FOR BUSINESS CHIEF MAGAZINE.
PUBLISHED BY:

BMG BizClik Media Group