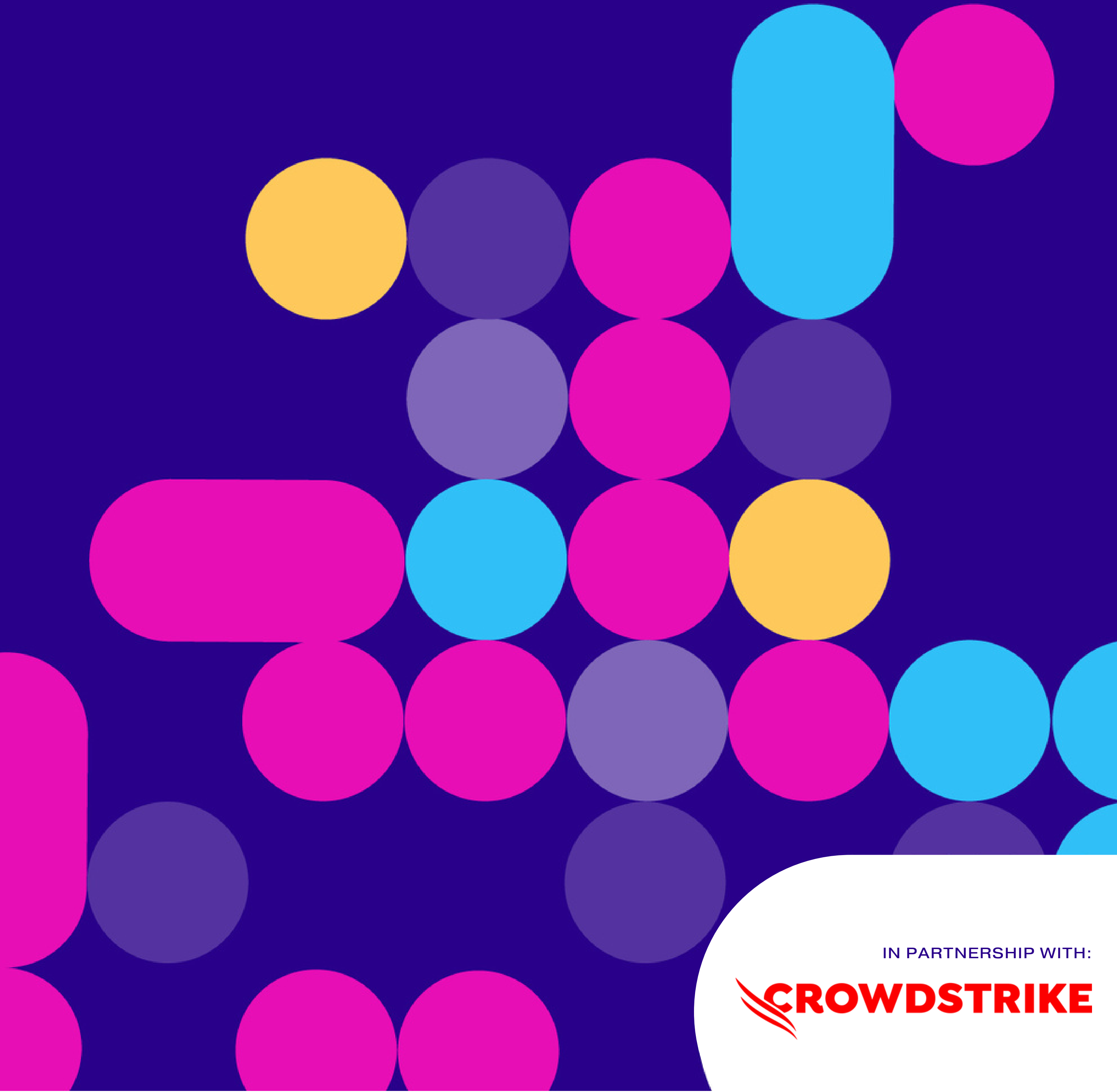
HotTopics

Prioritise, Protect, Personalise: Cybersecurity Strategies in a Dynamic Era



IN PARTNERSHIP WITH:

CROWDSTRIKE

Introduction

Over the course of 2023, many leaders within HotTopics' global community of CIOs, CTOs, CISOs, Chief Digital and Data Officers have voiced the admission that prioritisation is becoming harder than ever before.

And it isn't difficult to see why.

Global and regional market turbulence, rising inflation, remote and hybrid work, climate change, new customer behaviours and supply chain disruption all represent just a proportion of the trends executives are facing as headwinds. This is before they acclimatise to the present-day effects of generative AI, the medium-term range and effects of AI regulation, and the long-term impact of these technologies.

Where does cybersecurity fit in today's business world?

Cybersecurity fits everywhere, as it always should do. Yet the dynamics of security principles—and the reception of cyber as a keystone business strategy—have evolved in light of this poly-priority era. We know the Covid-19 pandemic accelerated better standards of remote and distributed models of security just as it raised the profile of the CISO and their teams. We also know that people, internal or external, benign or antagonist, remain the single biggest threat to businesses. And we now know that by and large, the Board is starting to comprehend the seriousness of the situation, catalysed in part by more technology leaders sitting on the Board, but so too the large-scale data breaches which make daily newspaper headlines. How these coalesce to impact organisations will depend fully on each organisation's size, sector, region and culture.

A CISO's responsibility has always been to protect the organisation based upon those contextual metrics. Given this dynamic era however, it is now one of three responsibilities: to prioritise the strategies vital to support the CIO and CEO, and to personalise them for the business' position; only then can they claim to protect.

FOOD FOR THOUGHT

To chart these three responsibilities, HotTopics invited 12 technology leaders to a private dining room in central London to share their insights, as part of its *Food for Thought* series that welcomes debate over a three-course lunch.

The following whitepaper distils a two-hour debate into key takeaways for fellow executives to learn, takeaway and action.

Thank you to following for their contribution to the debate and this whitepaper:

Technology leaders joining us:

- **John Spencer**, Director Sales Engineering - Northern Europe, **CrowdStrike**
- **Alan Crawford**, Director, **Technoivity**
- **Amitabh Apte**, former Global CIO, **Pet Nutrition, Mars, Incorporated**
- **Christopher Adjei-Ampofo**, CIO, **Uphold, Inc.**
- **Conor Whelan**, CIO & COO, **Experian**
- **Darren Desmond**, CISO, **Automobile Association Developments**
- **Georgina Owens**, CTO, 888, **William Hill International**
- **Giles Lindsay**, CIO, **Satago Ltd**
- **James Maunder**, Former CIO, **London Clinic**
- **Jots Sehmbi**, CIO, **City, University Of London**
- **Lee Fulmer**, Chairman, **Reporting and Data Standards Transformation Board, Bank Of England**

1. Facing external adversaries, insider threats

Organisations think they have a malware problem, but really, it may be more correct to say the industry has an adversary problem. Five years ago, the average breakout time for eCrime or adversary attack was nine-and-a-half hours, reported recently in a Crowdstrike report. Today, it is just 79 minutes. The fastest breakout time ever recorded is seven minutes. The window of opportunity to spot and remediate incoming threats has reduced dramatically.

Food for Thought guests heard in detail about the recent MGM cyber-attack in Las Vegas as a good example. Caesars' slot machines were taken offline, reportedly losing the company $4 million per day. Digital room keys were out of action for guests. The hackers were able to access personal information, including names, contact information, gender, date of birth, and driver's licence, passport, and even Social Security numbers, from "some customers" before March 2019, MGM said in a statement.

In this case, the attackers used social engineering, where attackers manipulate victims into performing certain actions by impersonating people or organisations with whom the victim has a relationship. To be specific, this was a case of "vishing," or gaining access to systems through a convincing phone call rather than phishing, which is done through email.

Food for Thought guests were reminded that identity threat, particular insider threat or inattention, remains the biggest concern for businesses and the executive team. In fact, 62 percent of interactive intrusions involve compromised identities in 2022, with 80 percent of breaches starting with identity management.

2. Engaging users in cybersecurity

Attack simulations and training

Leaders are prioritising cybersecurity awareness training and attack simulations to counter insider threats and external adversaries. Yet results often vary by organisational culture, and employee interest and engagement.

For instance, in attack simulations, leaders reported a counter-intuitive finding: the simpler the email phishing simulation, the more employees that would fall victim to the ruse.

“The more effort we put into making a sophisticated phishing template, the less people click it,” said one guest.

Security awareness campaigns meanwhile are often “incredibly dull”, and “don’t transfer across to people’s real lives”, which can result in awareness fatigue and disengagement, with *Food for Thought* guests pinpointing senior medical practitioners and university students as two particular examples.

“People value their own time, more than they value data and information security,” said one guest, when describing modern-day security awareness programmes.

Training, therefore, needs to be tailored to individuals. Which messages do each group need to understand? In what mediums are these best communicated? And how well do you know the behavioural characteristics of each cohort? These are just some of the questions security and technology leaders should now be asking themselves.

Culture and changing demographics

Security controls are tied to the culture of the organisation, as well as its region, sector and size, we heard. The CIO or CISO should understand how these contextual features impact those security controls, and align them to the businesses cyber priorities. Once this has been drafted, communicating this effectively to the CEO and Board is key; after all, senior leadership directly shape the culture of the organisation.

For some leaders, the younger generation - more technically literate but also more digitally exposed - represent the biggest demographic concern. For others, the reverse is true: older generations can be more cautious online but more resistant to change, a key barrier to the dynamic nature of cybersecurity and technology adoption more generally

Tailoring cybersecurity education based on persona may be a savvy next step for security leaders stumped for new ways to engage their teams.

3. New (and old) rules for security leaders

That led guests to debate to how leaders engage teams, or in other words, the art of storytelling.

Storytelling needs to connect teams and the boardroom. Crafting that story requires a clear understanding of business values, the different functions and disciplines within the business, and clarity on security's role in supporting the organisation in its objectives. It also requires human stories, aligned to real-world values. CIOs and CISOs should nurture their storytelling skills as a rallying point if they wish to instil confidence in their vision, their teams and even in themselves. But it can also shock or inspire, when done appropriate.

One guest recalled using an independent third-party, a penetration testing outfit, to perform a simulated attack. The third-party saw that the organisation was advertising new roles and so impersonated a candidate by applying for a position. The HR team were diligent at following the talent acquisition process but, upon receiving the CV, which contained the malware payload, opened the malicious file which gave the supplier access the company's systems.

"It was fascinating; it forced us to reconfigure our Microsoft System Center Configuration Manager (SCCM) because through that they were able to deploy payments to every single device in the company, which then cracked multi-factor authentication. In 24 hours, they could reach everything," said one of the guests.

In a former senior position at a financial services company, one of the guests protected innovation using sandbox methodology. To allow people to experiment, but remain protected, one team was taken off the corporate network and put onto a separate network which was completely isolated within the building. In fact, the team had to "pull up floor tiles and cut cables", so they could sit outside of the firewall. This provided an opportunity to work on new ideas, bring in new partners or vendors, and safely experiment. It meant anything in that space couldn't compromise the rest of the network, and was run successfully across three locations: London, New York and Singapore.

Sometimes, bolder, more creative ideas are needed. One guest could not get traction with the Board, with their security vision for the business. He paid a penetration tester to "attack" a Board member to prove how gathered intelligence via networks of family, friends and acquaintances can impact an individual. The idea was successful and the CISO soon found the Board more willing to listen to their plans.

An industry realignment?

During the conversation, we also heard the cybersecurity industry may need to realign on deciding between best-in-breed security tools, where each tool is best-in-class for its specific use case, and a platform approach that delivers a complete package of protection from a reduced number of suppliers.

The relative tension between CIO, CISO, CFO and cybersecurity vendor expectations should not be underestimated, however. CIOs and CISOs now need to be able to balance what exposure the CFO is willing to risk vis a vis the investment available—itself directly related to how well the CISO communicates the risks to the business—and what vendors are able to offer.

Do CISOs always want or need best-in-class cybersecurity? This debate challenged that assumption. Instead, a more pragmatic, personalised approach is desired by technology and security leaders to help them manage the relationship with the rest of the executive team as well as select the right controls to suit their business.

The importance of segmentation

Segmentation was brought up on a number of occasions throughout the debate. An effective technique to strengthen security, network segmentation is a physical or virtual architectural approach which divides a network into multiple segments, each acting as its own subnetwork providing additional levels of security and control.

This may cause friction between the CIO, whose teams want one system for efficiency, and the CISO, who is seeking to minimise risk. The latter needs to argue the segmentation case well, showing how parts of the business can be protected even during an attack happening elsewhere.

Security responsibilities

One of the biggest issues during a cyber-attack is not knowing who has control to make critical decisions. Is it the CISO? The CIO? The Head of Architecture or System Administrator? During those critical minutes of an attack, a breakdown in communication will compound an already serious situation. The single easiest thing to do today is agree upon who makes that decision and communicate that to all relevant stakeholders.

Another important consideration is asset management. Knowing what you have, and where it is, is half the battle in knowing what needs protecting and in what way. Visibility should be prioritised before spending any money.

4. Looking around and ahead

“Ivory tower policies”, or Board-directed security methodologies, remain a challenge for CIOs and CISOs, particularly within global and regional organisations. This type of top-down directive disregards the nuance of local markets and the importance of personalisation; in one such example, a guest remarked that his warehouses in India didn’t even have networks. Regional CIOs and CISOs must therefore understand what tools will best suit their business and communicate that back effectively to the global lead.

Resilience as a business concept will connect the CIO and CISO, bridging much-needed ground between their two departments. Resilience connects the availability piece that CIOs are concerned about with the data confidentiality and integrity that CISOs seek. Leaders recommended their peers to use this to streamline future senior leadership meetings, and improve alignment.

Looking ahead, *Food for Thought* guests discussed how cloud will become a new attack vector, “probably within the next 12 months.” The aforementioned Crowdstrike report found a 95 percent rise in cloud attacks between 2021 and 2022, and a 160 percent increase in credential theft via cloud instance metadata APIs. As businesses embark on new business models, which are increasingly reliant on as-a-service cloud architecture, how can leaders scale cyber ambitions inline with growth targets?

Elsewhere, government demands and AI’s profileration pose significant issues for technology and security leaders.

More governments want access to company data. The UK Government and Apple remain locked in a battle about whether to open or remain closed iMessages; when Blackberry acquiesced a similar demand from Saudi Arabia, the company soon folded. Educating governments on the realm of technology, innovation, privacy and security, particularly in relation to the IP of businesses, will be crucial in the future.

“Governments want better oversight of technology, without understanding what technology is,” remarked one guest.

Generative AI technologies are democratising chatbots, avatars and similar tools. How this will impact on a macro-scale questions of privacy and identity are difficult to quantify. It is a little easier to qualify: “Companies and industries are not prepared.”

Closing thoughts

For many, 2023 has crystallised certain long-term cybersecurity trends, such as the over-proliferation of tools, asset control and visibility, budget restrictions, and introduced still others, generative AI, geo-political headwinds and culture shocks.

For the CISO and CIO, it has never been more important to protect, or share best practices in a highly-changeable environment. The nature of how to protect is changing, however, becoming far more tailored, nuanced, even, to capture not just the market position of the business but the cultural parameters of the team.

Prioritisation and personalisation become integral here, then. Technology and security leaders need to better understand the business and become more confident in translating that into a strategy. That will determine not just what to prioritise, but how, and how often. This then personalises the plan to better protect the business and counter adversaries in 2023 and 2024.

Consolidate with Crowdstrike's Falcon platform to improve your security posture, increase operational efficiency and lower security TCO. Start your free trial today.

https://www.crowdstrike.com/

CROWDSTRIKE