Navigating a New Era for Cybersecurity

How Global Business Is Adjusting to the New Normal

Takeaways from Baird's 2021 Cyber Showcase

About Our Cyber Showcase

Baird's inaugural Cyber Showcase features in-depth discussions between Baird's Infrastructure Software & Cybersecurity Investment Banking team and leaders from compelling cyber solutions companies from across the globe.

Our discussions took place as global companies continue to navigate the realities of cyber threats in a world transformed by COVID-19. The shift to widespread remote work expanded the cyber perimeter in a major way, creating new threats and accelerating existing trends.

Our discussions confirmed the risks companies face today are global and industry agnostic. In the following pages, we highlight the key takeaways from cyber leaders who are working closely with global companies facing the new normal in cybersecurity.

Participating Companies

ADARMA

The UK's largest independent security services company
John Maynard, CEO

CybelAngel

Leading digital risk protection platform
Camille Charaudeau, VP, Marketing & Product Strategy

GUARDSQUARE
Mobile application protection

Leader in mobile application protection
Roel Caers, CEO

MALTEGO

Open source intelligence and graphical link analysis tool
Philip Mayrhofer, CEO

ORPHEUS

Premier threat intelligence and cyber risk rating provider
Karla Reffold, COO

Outpost24

Leading cyber assessment company
Bob Egner, CMO

S-RM

Global intelligence and cyber security consultancy
Heyrick Bond-Gunning, CEO

Key Takeaways

See the following pages for in-depth insights on each takeaway

1	**Security Starts & Ends with People**	Humans are the first line of defence and point of vulnerability – and the pandemic environment put pressure on both roles
2	**Familiarity & Shadows Hide Vulnerabilities**	Lack of visibility into attack surface, assets, legacy stack and more creates significant risk in today's cyber landscape
3	**Supplier Risks Are More Dynamic Than Ever Before**	Point-in-time questionnaires no longer cut it – continuous monitoring is essential as third- and fourth-party risks ramp up
4	**Remote Working, Rich Pickings**	Work-from-home created a ripe environment for threat actors, with malware, phishing and mobile attacks all on the rise
5	**Low Visibility – IT Ops Navigating Cloudy Skies**	Teams are navigating a myriad of challenges around cloud migration, data storage, non-integrated datasets and more
6	**Regulation Looms**	Ransoms remain a big question mark for regulators, and GDPR stands to re-emerge as a concern for businesses
7	**Shoring Up on Cyber Hygiene**	Businesses must develop good cyber hygiene habits – and proper awareness, processes and training will be key

KEY TAKEAWAY #1:

Security Starts & Ends with People

Humans are central to cybersecurity, providing frontline defence and often serving as the first point of vulnerability for malicious attacks. COVID-19 presented threat actors with a unique opportunity to execute cyber attacks through the rapid rise of a work-from-home paradigm. This confluence of trends expanded the cyber perimeter, creating novel cybersecurity challenges, straining IT teams, and upending traditional practices and processes in a matter of weeks. Simply put, more people online, in a distributed model, created more opportunities for hackers to launch malicious attacks. Ransomware in particular has emerged as a significant, growing threat to businesses.

70%

Cybersecurity professionals who are approached by recruiters at least once a month[1]

38%

Estimated increase in cyber insurance and reinsurance premiums, 2021-23[4]

Key Takeaway #1: Security Starts & Ends with People

Cyber talent shortage

"There's a shortage of cybersecurity talent. So, focusing on your cybersecurity hygiene process, focusing on having the talent and knowledge that's necessary to be able to understand your exposure and put some control around the exposure, is really the biggest gap that we see across the industry today."

▶ *Bob Egner, Outpost24*

What's the role of machines in the talent shortage?

"Generally, I think, just the case load is increasing – the number of data sources, data in general, the amount of data is increasing. At the same time, machines cannot solve it all. But you still have, especially for the exploratory searches, you need this fuzzy intelligence and that's what the human can bring to the table."

▶ *Philip Mayrhofer, Maltego*

Robots aren't the full answer

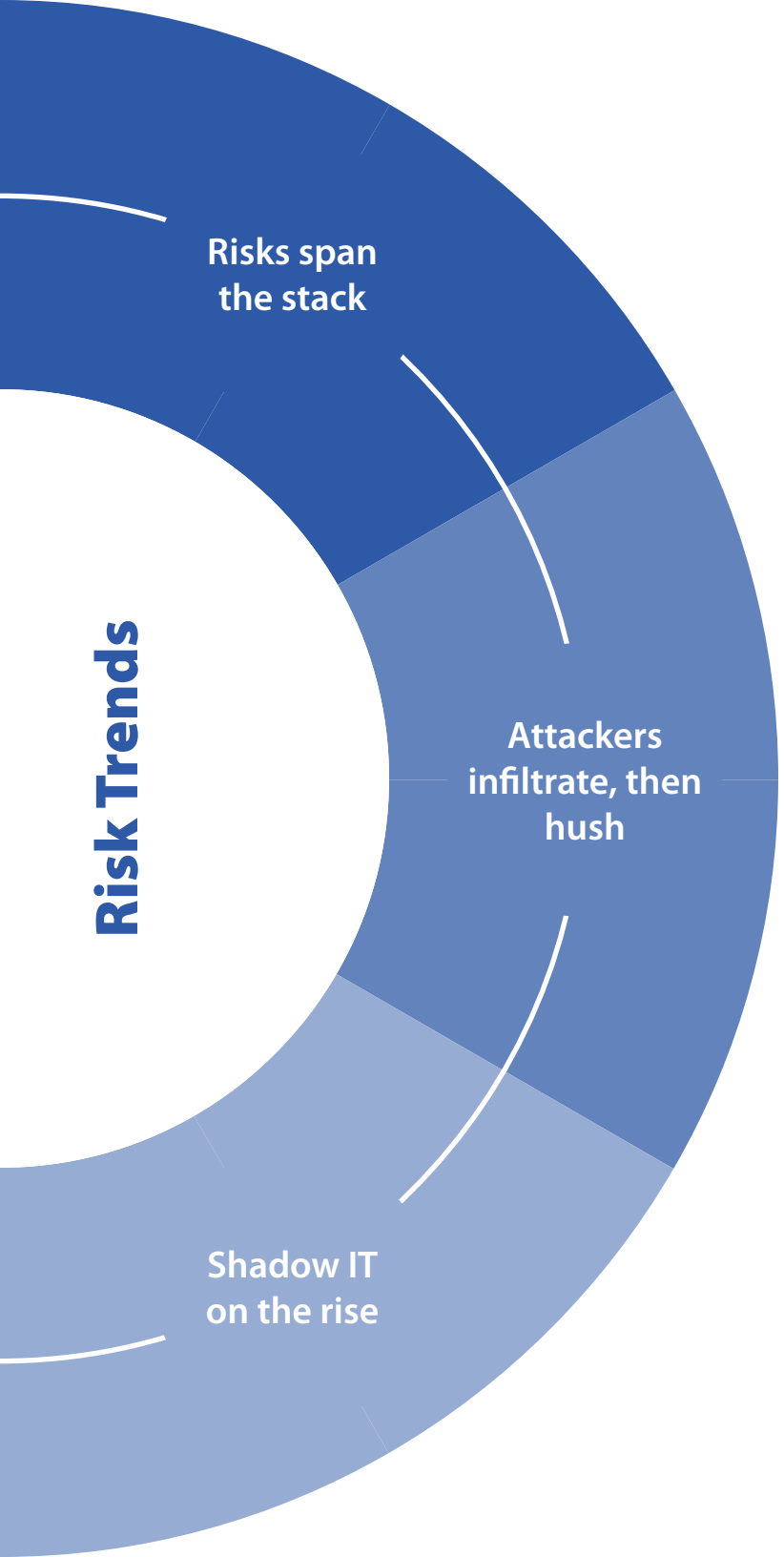
"We believe AI, machine learning, automation is only part of the puzzle. It's not the rise of the robots - it's not going to extinguish the need for people. It is a solution to the problem of the skills gap. And automation and AI and machine learning helps with that skills gap, but we've also got to understand it can be used against us."

▶ *John Maynard, Adarma*

KEY TAKEAWAY #2:

Familiarity & Shadows Hide Vulnerabilities

Businesses need, but often lack, a thorough understanding of their company's potential attack surface and all that sits within their estate. Without this robust visibility, companies do not know how they can be attacked, where they can be attacked or what tools they'd need to preempt an attack. Threat intelligence, assessment tools and cyber risk consultants have become prominent in this space to identify vulnerabilities and develop a cyber posture tailor-made for each company.



Key Takeaway #2: Familiarity & Shadows Hide Vulnerabilities

New environment, new dangers

"The threat landscape increases in velocity in terms of the orchestration and the organization of the adversarial landscape…transitioning from an office-based hybrid location to really having everyone working at home, accessing applications off network, on or off corporate-owned devices, fundamentally has changed the way that we think about the attack surface, the expansion of the attack surface, and really the acceleration of digitisation in a very, very short space of time."

▶ *John Maynard, Adarma*

Legacy infrastructure is prone to exposure and leaks

The legacy stack "[has] really been exposed, and we hear it a lot by organisations telling us that some of their technology is being decommissioned or it's something that they don't use."

▶ *Karla Reffold, Orpheus*

Shadow IT presents a major risk

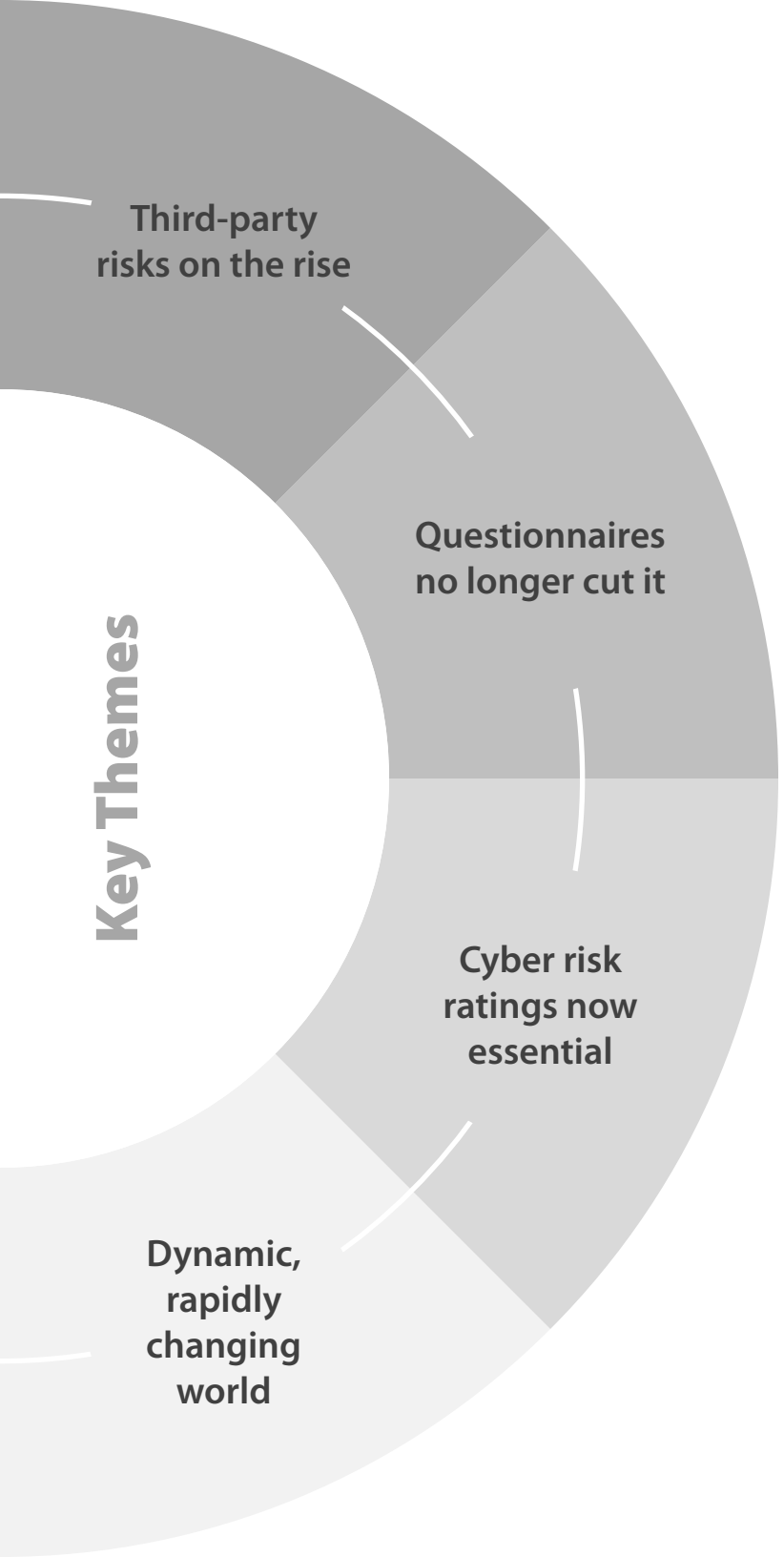
"Really, the heartbeat is that visibility component…most of that is shadow IT. Those manufacturers don't even know that these assets can put them at risk and are vulnerable."

▶ *Camille Charaudeau, CybelAngel*

KEY TAKEAWAY #3:

Supplier Risks Are More Dynamic Than Ever Before

The pandemic environment continues to strain the global supply chain, forcing companies to be more agile in resourcing – and creating new cyber risks specific to engaging with suppliers. Traditional onboarding questionnaires are no longer sufficient to vet vendors and supply chain participants. While the questionnaire tool has long been used by companies to evaluate a vendor's cyber hygiene and internal risk protection procedures, it provides a point-in-time assessment and does not account for the changing cyber landscape. This creates a need for continuous monitoring and dynamic risk ratings, the latter of which is becoming a more prominent tool to evaluate third- and fourth-party vendor risks within company supply chains. While it is difficult to keep up with this rapid pace of change, global business must continue to shift to a more dynamic model of monitoring supply chain risk.



Key Takeaway #3: Supplier Risks Are More Dynamic Than Ever Before

Small companies aren't immune to hackers

"They're interested in your clients and they're using you and your lack of security to gain a foothold into those organisations."

▶ *Karla Reffold, Orpheus*

Supplier breaches are ramping up

"More than 60% of companies have already been targeted by a third-party breach, and that will keep on growing. I would say that the bigger and broader your ecosystem of partners, suppliers, and customers is, the bigger you are exposed to those new cyber threats we're just discussing. The more global the business, the greater the risks."

▶ *Camille Charaudeau, CybelAngel*

Can you count on your software vendor?

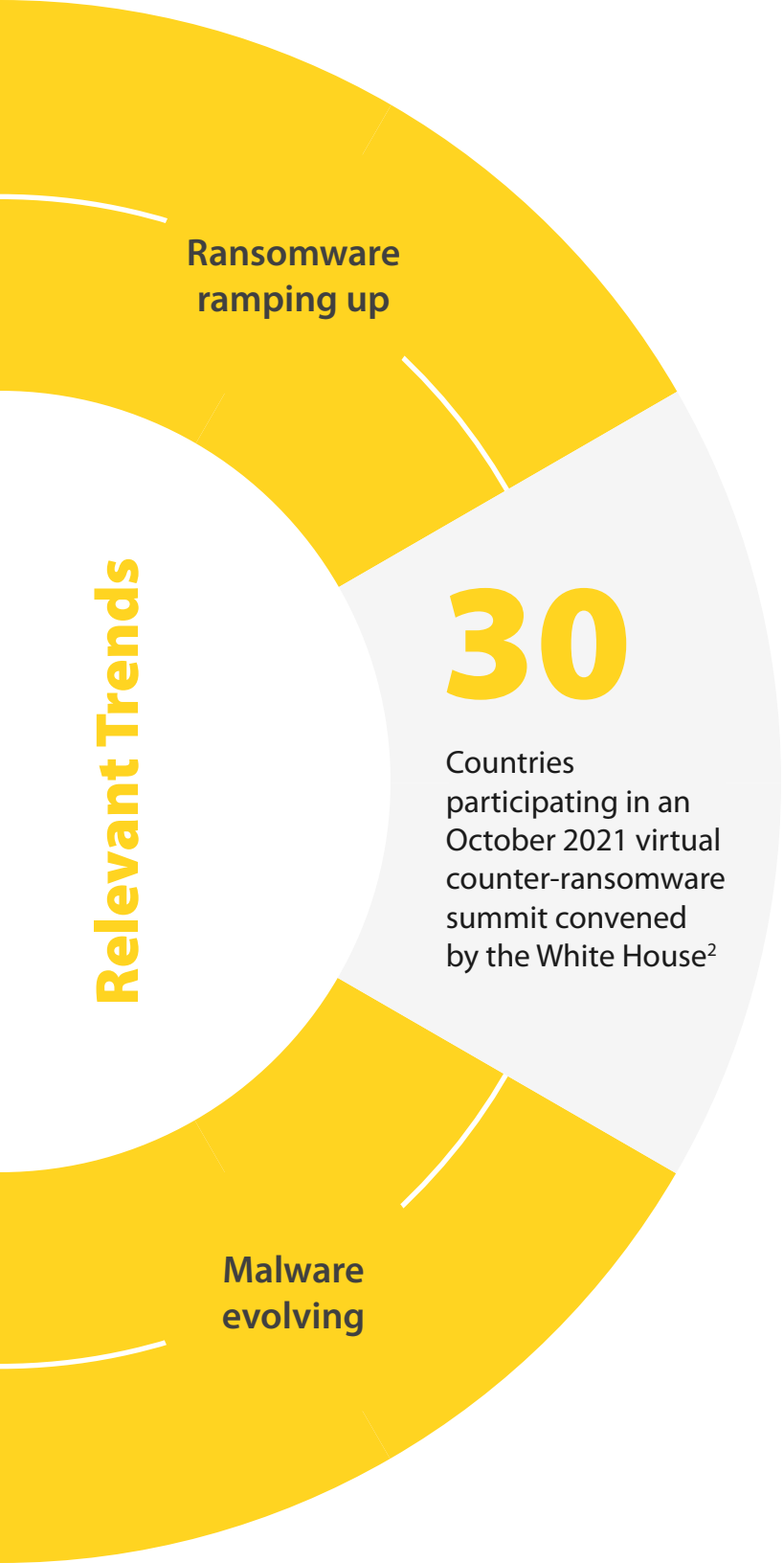
"There are a lot of interesting new attack vectors that we've seen hit the market recently. For example, software supply chain – for an attacker to try to inject themselves into the software update techniques that are used by a lot of tech companies has created a wealth of new attack vectors that companies…in the past, they were just assuming they were secured by the software vendors that they were working with."

▶ *Bob Egner, Outpost24*

KEY TAKEAWAY #4:

Remote Working, Rich Pickings

Hackers are finding innovative ways to exploit the new normal, and attack numbers are on the rise. The volume and financial impact of cyber attacks has ramped up since the pandemic disrupted the market: "I think there's been an 85% increase in phishing attacks targeting remote enterprises, and around a 33% increase in the average ransom payment," said Heyrick Bond-Gunning, CEO of S-RM. Our discussions also underscored hackers' continued drive to access information in new ways and in new end markets.



Key Takeaway #4: Remote Working, Rich Pickings

Malware techniques are evolving and commoditising…

…causing exponential growth and availability of ransomware - "effectively, ransomware as a service."

▶ *John Maynard, Adarma*

Gone phishing

"It's not just the big attacks like the ones we think about from nation-state actors. It's actually a volume game still. When we talk about phishing, as you know, it's so easy to get a large amount of people out of all these millions of people out there, and one makes a mistake leading to a compromise and possibly ransomware."

▶ *Camille Charaudeau, CybelAngel*

Mobile increasingly a target

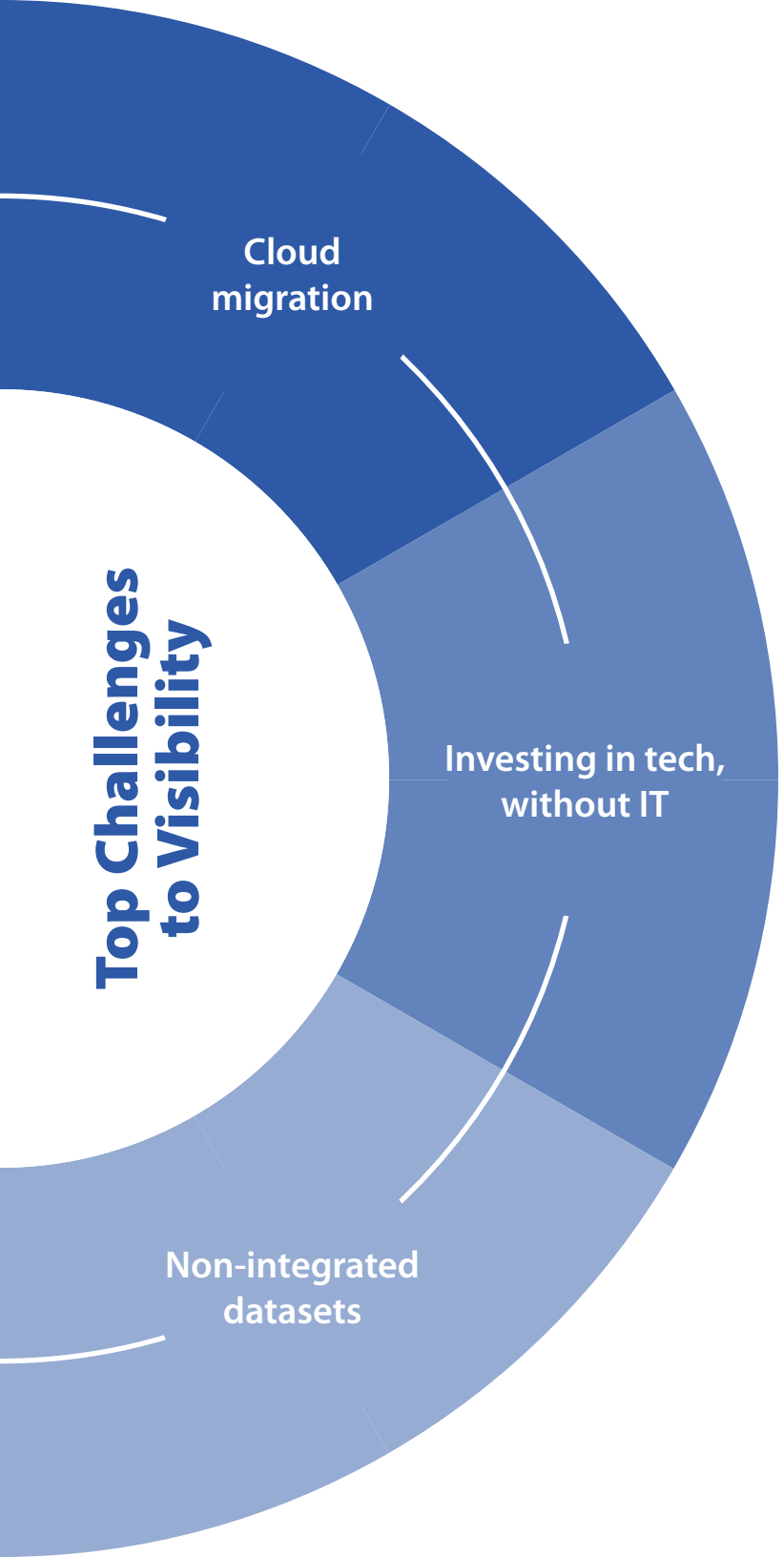
"There are more and better tools available for hackers or people who want to do malicious things, while too many apps on the other side are still without any defence. So if you don't protect your apps and you know that all these tools are available on the Internet and can be easily used, the question is not will, but only when your application will be hacked…so, think about an app with sensitive data or money in there, it is a risk, and if it's not protected, it will be attacked…aside from finance, there's ecommerce, there's healthcare, there are the telcos, all streaming-like media, streaming services – across the globe. They are all high at risk and they know."

▶ *Roel Caers, Guardsquare*

KEY TAKEAWAY #5:

Low Visibility – IT Ops Navigating Cloudy Skies

The rise of COVID-19 created new visibility challenges for many companies. To support the vast, fast shift to remote work, many cybersecurity teams were pulled out of their normal functions and thrust into operational roles to support a newly distributed workforce. Cloud migration presents another significant visibility challenge, as it can make it difficult for companies to keep up with the storage of sensitive information and the control of data and assets being added to cloud environments.



Key Takeaway #5: Low Visibility – IT Ops Navigating Cloudy Skies

DevOps must lead with Security

"So specifically at their software development life cycle, at the CI/CD development chain within the DevOps process, to make sure that security is built in as part of that process, and that we have the right checks and balances given the speed at which these are then put into production in the cloud environments."

▶ *John Maynard, Adarma*

Going on offense to regain visibility

"Pre-COVID, teams used to control what we would call the perimeter. And now it has literally exploded, exponentially exploded. So, there is clearly now a lack of visibility in this new extended ecosystem…how do we gain back that visibility and control and how [do] we not just wait for the attacks to happen in this new environment? There is a shift toward a proactive mindset or proactive approach."

▶ *Camille Charaudeau, CybelAngel*

Vendors' cloud security matters, too

"We actually saw a lot of the large data breaches happening over the past couple of years in 2019 and 2020 coming from exactly this scenario, unprotected buckets of data that were available on the cloud, were set up by a marketing agency without the correct security controls, and that data was stolen in a very short timeframe. So, the results, the consequence, of course, is a big data breach. It's bad for reputation, it's bad for the customer relationship, but it's a great example of putting technology in the hands of people who are maybe not thinking about all of the dimensions of how technology should be used."

▶ *Bob Egner, Outpost24*

KEY TAKEAWAY #6:

Regulation Looms

The biggest unresolved question in cybersecurity is what will happen with cyber insurance and ransomware regulations. Ransomware attacks on critical utilities in the U.S. have increased concerns about cybersecurity across Europe and the globe. Since critical utilities and major multinational companies have been targeted by these attacks, regulation is likely soon to follow. One possibility is a shift in government policies to better police and control what can and cannot be paid for ransoms. Additionally, as regulations start to harden for those companies, cyber insurers will need to re-think how to cover those attacks – or whether they will be able to provide coverage in the future as the volume of attacks continues to mount.

GDPR is also poised to re-emerge a force in the market. A number of significant GDPR fines have been rendered against major companies in recent months, and the legislation will continue to be front-of-mind for companies and regulatory bodies.

Nearly

$600 million

Value of suspected ransomware payments reported by U.S. banks in 1H 2021, exceeding 2020's year-end total[3]

Up to

100% increase

Estimated increase in cyber insurance and reinsurance premiums, 2021-23[4]

Key Takeaway #6: Regulation Looms

Ransomware must be checked

"Threat actors are always one step ahead. Ransomware is clearly problematic and that's going to start affecting more and more organisations, particularly as the larger organisations put solutions in place that make it harder for those criminals to breach them and to affect them with that."

▶ *Karla Reffold, Orpheus*

Regulation will force a focus on cyber resilience

"There's probably going to be some form of governmental regulation around paying ransom – i.e., you're not allowed to or…you're not allowed to insure against it, and so we're going to end up with companies having to really focus on their cyber resilience."

▶ *Heyrick Bond-Gunning, S-RM*

KEY TAKEAWAY #7:

Shoring Up on Cyber Hygiene

Cyber hygiene is more important than ever before, and it's an area where many organisations need specialised expertise. Showcase participants confirmed the need for comprehensive technologies, talent and processes to manage an organisation's cyber exposure and overall cyber health. Dynamic protection is essential to cyber hygiene. Leaders must continue to increase cybersecurity awareness among their employees, as well as drive improved processes and training to enhance and maintain security in the future. It is vital to understand and take steps to secure both upstream vulnerabilities – for example, security in the DevOps phase – as well as downstream vulnerabilities like third-party risks and risk ratings findings.

In short, constant monitoring is no longer a nice-to-have: It's a must-have for companies in the current environment. Point-in-time assessments are simply no longer sufficient in a world of constantly evolving software and cyber threats. As more and more software is pushed out, more and more security vulnerabilities will emerge. Growth in software will naturally perpetuate the cybersecurity cycle, and businesses must strive to build the right processes and technology to support constant monitoring and evaluation.

$4.24 million

Average cost of a data breach globally, up nearly 10% over 2020[5]

Key Takeaway #7: Shoring Up on Cyber Hygiene

Not a single-note issue

"I think the horror stories really come as you start to think about technology only, or you think about people only. It really is people, process and technology that need to operate in unison in the security world."

▶ *John Maynard, Adarma*

A unified front is key for preparedness

"I think a healthy way to look at an organisation's cyber stance is to think of it like three legs of a stool – the people, the processes and the technology, and not trying to rely on just one of those things, because all three are super important in terms of trying to support the company and prevent them from having some form of cyber attack."

▶ *Heyrick Bond-Gunning, S-RM*

The ultimate defence equation: Humans *plus* machines

"If you rely heavily on automations, on rules at detecting threats or intruders that are trained on historic data, and all of a sudden you have a major categorical shift in the landscape that actually lead to new and categorical changes, those machines sometimes maybe are not calibrated that well in the beginning. And that also obviously is then where the human needs to come in and try to navigate this."

▶ *Philip Mayrhorfer, Maltego*

Get a Deeper Download

Baird's Technology & Services team combines global capital markets capabilities with extensive industry knowledge to offer leading M&A advisory and capital-raising services. Deep sector-specific domain expertise enables our Technology & Services team to offer insightful, value-added advisory services to middle-market clients seeking to raise capital or consider strategic alternatives.

Baird's Infrastructure Software & Cybersecurity team has an extensive breadth of experience as investors in and advisors to the sector. Our sector expertise covers on-premise and cloud networking solutions, network security, outsourced IT services and cloud implementation and managed services. Our middle market focus and reputation of transaction execution excellence enable our team to deliver a great outcome for your company.

Infrastructure Software & Cybersecurity Team

Europe

Simon Pearson
Managing Director
+44-207-667-8409
spearson@rwbaird.com

Justin Prichard
Managing Director
+44-207-667-8524
jprichard@rwbaird.com

Chelsea Smith
Vice President
+44-207-667-8342
cmsmith@rwbaird.com

Marine Dumoulin
Associate
+44-207-667-8363
mdumoulin@rwbaird.com

North America

Craig Rogowski
Managing Director
+1-650-947-6815
crogowski@rwbaird.com

John Song
Managing Director
+1-703-394-1832
jsong@rwbaird.com

Evan Mueller
Director
+1-503-273-4956
emueller@rwbaird.com

Learn more at: techservices.rwbaird.com/cybershowcase

[1]CSO, "7 key data points on the cybersecurity skills shortage." 19 August 2021. Accessed via https://www.csoonline.com/article/3629460/7-key-data-points-on-the-cybersecurity-skills-shortage.html

[2]The White House, "Background Press Call on the Virtual Counter-Ransomware Initiative Meeting." 13 October 2021. Accessed via https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/

[3]Financial Crimes Enforcement Network, "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021." Accessed via https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

[4]S&P Global Ratings, "Cyber Risks in a New Era: Reinsurers Could Unlock The Cyber Insurance Market." 29 September 2021. Accessed via https://www.spglobal.com/ratings/en/research/articles/210929-cyber-risks-in-a-new-era-reinsurers-could-unlock-the-cyber-insurance-market-12118547

[5]IBM Security, "Cost of a Data Breach Report 2021." Released 28 July 2021. Accessed via https://www.ibm.com/security/data-breach