Cyber Risk Trends for 2023:

What You can do Now to Protect Your Operations

Chris Burrow and Jesper Sahlberg
January 26, 2022

Global events ranging from war in Ukraine, hyperinflation, rising interest rates, climate change, predictions of a possible economic recession, and cyber threats will continue to make headline news in 2023. Managing these threats will be a significant focus within C-Suites domestically and internationally.

Cyber incidents will continue to be one of the most immediate threats to organizations large and small, particularly given the costs of paying ransoms, business interruption, remediation, reputational damage, and potential litigation. Cybercrime is projected to reach $8 Trillion in 2023 according to a recent report by Cybersecurity Ventures (1). If it were measured as a country, cybercrime would be the world's third largest economy after the U.S. and China!

Why do cyber-crimes continue to climb?

In a recent article, McKinsey & Company has examined several of the latest cybersecurity trends as well as their implications for organizations facing growing cyber risks. "The rate of change is accelerating. Companies are continuing to invest in technology to run their businesses. Now they are layering more systems into their IT networks to support remote work, enhance the customer experience, and generate value, all of which creates potential new vulnerabilities (2)" according to their examination.

In a recent report and survey conducted by PwC, senior executives who were surveyed worry their enterprise isn't fully prepared to address heightened cyber risks. Topping PwC's 2023 list of rising organizational threats are cybercriminal activity (65% of those surveyed); mobile devices (41%); email (40%); cloud-based breaches (38%); business email compromise/account takeover (33%); and ransomware (32%) (3).

Fortunately, there are a number of immediate action steps and measures organizations can implement now to help reduce the chance of a crippling cyber breach. We're providing some predictions about the potential

source of cyber threats in the new year – and what leadership teams can do now to mitigate these cyber risks. Our prediction of trends is based on our conversations with countless C-Suite leaders as well as the collective observations of leading consulting firms and advisors in the U.S. and abroad. We have narrowed these threats down to the major cyber risk trends for 2023.

1. A Broader Focus on Cyber Risk Quantification Within Organizations

Organizations which have maintained successful cyber risk practices first define the scope of their risk exposure and quantify the level of risk. This allows them to establish their cyber risk management objectives. They begin by evaluating how cyber risk information is gathered and how they decide on counter measures. These organizations assume a risk-based approach which focuses on the most important assets and the biggest, most probable threats.

Quantifying an organization's cyber risk is key to making informed decisions about addressing - and reducing significant risk and developing a strategy to manage that risk on an on-going basis. It is essential to share this strategy with the entire leadership team including the CEO, CFO, legal counsel, Board, and all others.

Without a concrete quantification of cyber risk in financial terms, leadership will struggle to allocate funding that properly safeguards their assets. An organization should adopt a solution that provides clarity of their cyber risk exposure and the financial impacts so the best management decisions can be made.

According to John Chambers, the founder of Cisco and JC2 Ventures, cybersecurity risk management is at a crossroads. He recommends increased use of cyber risk quantification in order to achieve a reasonable cyber risk posture. "What was once considered a nice-to-have cybersecurity solution has now reached the inflection point of becoming a must-have cybersecurity solution – because cyber risk quantification is the foundation for addressing the most critical concerns about a business' cybersecurity posture," Chambers wrote in a recent article for TechCrunch (4).

Quoting the "Cost of a Data Breach Report," the most impactful methods to minimize dollar value losses include security AI and automation, Incident Response (IR) planning, and risk quantification techniques. "Risk quantification and management platforms consolidate telemetry signals from a business' attack surface and continuously update its cyber risk posture through data-science based algorithms," states Chambers.

2. Increasing Engagement by the C-Suite

In today's high-risk environment, addressing cyber risk at the leadership level is of utmost importance. The leadership team must recognize cyber risk as a business problem, not just an IT problem. Cyberattacks jeopardize business assets and, by extension, the financial livelihood of the entire enterprise.

Corporate leaders should work as a team and demand a holistic and objective examination of both their internal and external threat environments so they can properly quantify their organization's cyber risk. The resulting business metrics and supplemental insights will steer leaders to make the best cyber risk management decisions for their organizations, thereby demonstrating due diligence and minimizing their potential financial loss.

The level of cyber threats and their accompanying costs as well as the interruption of critical business operations will increase the level of engagement by the C-Suite in 2023. New initiatives launched in the new year will, unfortunately, be exposed to the same risks of the entire organization. Whether it is a key merger or acquisition, introducing a new product, or the entrance to a new market – the success of all will be subject to potential cyber risks.

C-Suites are taking bolder approaches to lead in the area of cyber risk management, according to PwC's Global Digital Trust Insights 2023. Corporate leaders are beginning to "step out of their independent cyber-specialist role and into one of partnering with not just a few executives, but the entire C-Suite. These collaborations have never been more critical."

Key findings of the PwC study include the following:

- Forty-two percent of senior executives say cyber breaches of their systems have increased since 2020.
- More than a quarter have had a consequential data breach in the past three years costing more than $1million. At least 10% suffered costs of $10 million or more.
- To CFO's, the most devastating consequences when a breach occurred were:
    - ✓ Downtime or disruptions in productivity
    - ✓ Damage to service and product quality
    - ✓ Lost contracts and business opportunities

CEO's who have suffered breaches within their organizations are particularly determined to accelerate their management of cyber risk. They want more information to help them make informed decisions to oversee their organization's cyber risk exposure. And they want to report more fully and in more detail to their boards and constituents as to exactly what measures are being taken, according to the PwC report.

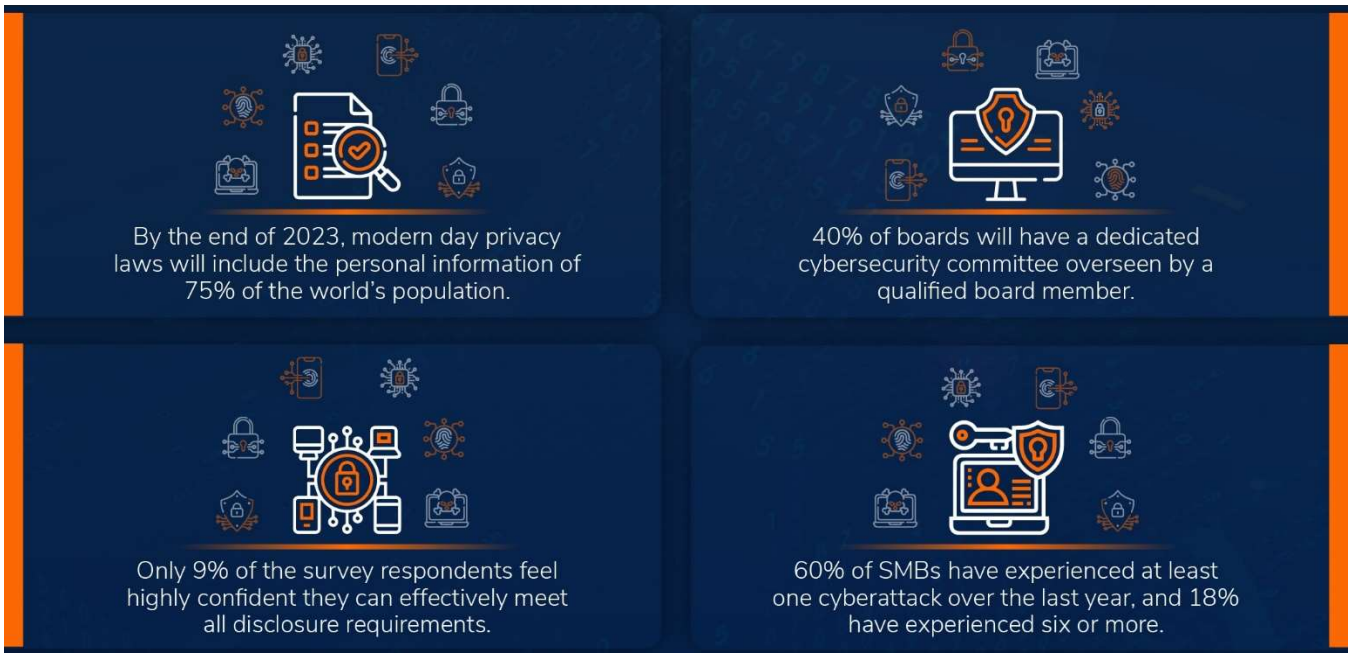
3. More Rigorous Board Oversight

As the cyber threat landscape continues to evolve and become more sophisticated, "the role of the Board of directors in cyber risk oversight is becoming increasingly important," according to Deloitte. As organizations focus on continued growth while maintaining customer trust, "the Board can help position Cyber as a strategic enabler to foster stronger relationships among customers, vendors, employees, and shareholders" (5).

Due to these factors, security and risk management have become a priority for board-level oversight with many organizations. Security breaches are not only becoming more common, but are becoming more complex as well. As a result, new laws are being passed to protect consumers and companies.

Most organizations focus on cyber protection rather than cyber resilience, according to a recent article in the *Harvard Business Review*. "Resiliency is more than just protection: It's a plan for recovery and business continuation." "Being resilient means that you've done as much as you can to make sure you can continue to operate when an incident occurs" (6). Based on the Harvard supported research, most board members believe it's not just a matter of if, but when their company will experience a cyber event.

"Our research indicates that boards are hearing about cybersecurity from management but the discussions must take place more often. It's not a 'one and done' type of decision: cybersecurity is a continuously changing and moving target. The more often the board is exposed to the cyber-situation of their organization, the more comfortable and more expert they become."



These trends put security at the center of corporate and board decisions, according to predictions for 2023 – 2025 developed by Gartner (7). By 2025, according to the Gartner report, 40% of boards will have a dedicated cybersecurity committee overseen by a qualified board member. Such a board level committee "increases the visibility of cybersecurity risk across the organization and requires a new approach to board reporting."

"We're falling into this old habit of trying to treat everything the same as we did in the past," Gartner Analyst Sam Olyaei said in his presentation at the Gartner IT Symposium 2021 regarding this topic. "This simply cannot continue. We need to make sure that we are evolving our thinking, our philosophy, our program, and our architecture."

4. A More Complex Regulatory Environment

By the end of 2023, modern day privacy laws will include the personal information of 75% of the world's population, according to the Gartner report. New regulatory mandates are emerging rapidly.

Meanwhile, the US Securities and Exchange Commission is considering a rule that will require publicly held companies to disclose their cyber risk management, strategy, governance and "material" cyber incidents. Specifically, where pertinent to board oversight, publicly traded companies will be required to disclose:

- Whether the entire board, a specific board member, or a board committee is responsible for the oversight of cyber risks;
- The processes by which the board is informed about cyber risks, and the frequency of its discussions regarding cyber risks;
- Whether and how the board or specified board committee considers cyber risks as part of its business strategy, risk management, and financial oversight.

The scope and reach of these regulations are forcing corporate leaders to manage multiple data protection laws in multiple geographic regions. On the regulatory front, only 9% of the PwC survey respondents feel highly confident they can effectively meet all disclosure requirements – even as pressure mounts from regulators to report cyber incidents.

Also, customers are increasingly demanding information on what kinds of personal data is being collected from them, with what groups that data is being shared, and how it is being used. “This means that you need to focus on automation of your data privacy management system. As for how to do this, basically using GDPR, you can standardize security operations and then tailor it to individual jurisdictions,” according to the study.

5. More Attacks Targeting Smaller Companies

Cyberattacks are not limited to large organizations. Over 60% of SMBs have experienced at least one cyberattack over the last year, and 18% have experienced six or more. Midmarket companies are targeted by criminals today more than ever before. Unfortunately, this is expected to only increase in 2023, and beyond. Fast growing smaller organizations are exposed to proliferating digital touchpoints,” according to the McKinsey report. Malware such as ransomware is a growing threat to small and midsize businesses (SMBs) and midmarket companies and have a more dramatic impact.

Midmarket entities are often targeted by criminals looking to exploit unsophisticated security tooling. With the proliferation of ransomware attacks targeting SMBs and midmarket companies, such companies have a responsibility to address cyber risk exposure – even if they don’t currently employ or engage a security team.

6. Cyber Attacks as Acts of War and State Sponsored Cyber Events

State sponsored cyber attacks are on the rise. State sponsored attacks threaten to wreak havoc on companies’ essential IT systems, Internet devices, software, and all manner of critical infrastructure housed in private sector hands, according to Sidley. Nation state sponsored attacks tend to be highly sophisticated compared to typical breaches such as ransomware attacks.

The Colonial Pipeline ransomware attack in May 2021 was a wakeup call around the globe. It was the largest such breach of an oil infrastructure operator in U.S. history. As the largest supplier of gasoline and jet fuel serving the Southeastern U.S., the breach forced the shutdown of the entire pipeline system. The operator paid $4.4 million in ransom demands. The FBI identified the Russian criminal hacking group “DarkSide” as being behind the attack.

State sponsored cyberattacks are characterized by the following:

- The level of sophistication can range from a complicated botnet to launch DDoS attacks to supply chain compromises.
- The response to a state-sponsored hacking routinely requires close coordination with multiple U.S. and foreign government agencies.
- State-sponsored threat actors often target companies running outdated software containing previously identified and publicized vulnerabilities.
- State-sponsored threat actors may be politically motivated, and their goals may not be clear and can change over time.

In March of 2022 the White House issued a stark warning based on “evolving intelligence” about potential Russian cyberattacks on the United States in response to U.S. – imposed economic sanctions. The private sector

was specifically warned that the Russian government may target companies that operate critical infrastructure. In response, the Biden administration has made cybersecurity defense a key agenda item.

In July of 2021, the National Security Agency (NSA), along with the FBI, determined that China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets. In March, 2022, Congress passed the Strengthening American Cybersecurity Act, which will require critical infrastructure entities to report cyber incidents within 72 hours, and ransomware payments within 24 hours, to CISA (Cybersecurity and Infrastructure Security Agency). These measures make it quite clear that nation-state cyber-attacks can be highly sophisticated and difficult to address.

7. A More Challenging Cyber Insurance Marketplace

The cyber insurance marketplace is complex and confusing and a sector in the insurance industry that is still in its infancy. Cyber insurance, therefore, is evolving rapidly in terms of its availability, pricing, limits, and exclusions. The cyber insurance marketplace is also highly volatile. According to Tom Johansmeyer writing in the *Harvard Business Review*, "while more attacks could stimulate demand, they also create a supply problem, making insurers warier of providing coverage and reinsurers less interested in backing cyber liabilities. On top of that, the lack of historical loss data adds another layer of unpredictability for all involved" (8).

Cyber insurance is becoming more costly by the month, limits are being reduced, and exclusions are being expanded. It's possible that cyber insurance could become prohibitively expensive for many companies or the option for cyber insurance could be lost altogether. That would be the loss of an important risk transfer vehicle for organizations with significant technology exposure.

According to a recent report by Gallagher, "carriers have been under pressure due to the increasing frequency and severity of cyber claims and a rapidly expanding regulatory environment at the state, federal and international levels" (9). As a result, there will likely be a reduction of capacity in the market, which will likely continue to increase pricing. Some industries are already seeing significantly higher premiums and a "pulling back" from high-risk industries all together[7].

Summary

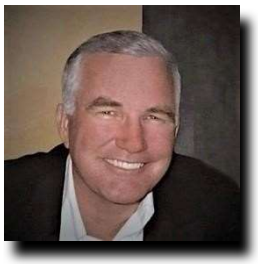
In 2023 reputational consequences from cyber incidents will be bigger than ever before. Regulatory requirements for safeguarding data privacy are now agnostic to both industry and company size. Third party cyber risk from your supply chain will continue to increase both as the root cause of cyber incidents as well as increase the financial, disruption and reputational impact on your organization.

The Biggest cyber risk in 2023? How you chose to identify and quantify cyber risks.

Most important cyber risk decision in 2023*?* How you chose to manage cyber risks, on a continuous basis, and aligned with the dynamics of and innovation pace within the cybercrime industry.

Most preventive effort to protect company reputation and valuation? Establish a robust cyber risk registry to defend company and fiduciary leadership against future negligence claims.

About the Authors



Chris Burrow is a Partner and Senior Strategic Advisor at Maxxsure Cyber Risk Management based in Addison, Texas. Chris has served in CEO, CFO, COO, and board positions in both for-profit and non-profit organizations for over 30 years. Those include organizations in the real estate services and advisory sectors as well as educational institutions and foundations. Chris enjoys cycling, golf, mountain climbing and business writing in his spare time.

chris.burrow@maxxsure.com

Jesper Sahlberg is the Chief Technology Officer & Executive Cyber Risk Advisor at Maxxsure. Sahlberg was previously CISO & VP of IT/Technology at Assima Inc. Sahlberg received his Bachelor's/HA in Economics from Copenhagen Business School and has has served on the Board of Directors of the Danish American Chamber of Commerce and holds a license in competitive road racing from NASA (National Auto Sport Association).

Jesper.sahlberg@maxxsure.com

About Maxxsure

Maxxsure is a cyber risk quantification, management and advisory firm based in Addison, Texas. The firm's services and proprietary management platform enable clients to confidently identify, quantify and manage cyber risk.

The firm's customers include global industry leaders in commercial real estate services and investments, financial services, law, ratings, gaming, wealth management, telecommunications, and data management, to name a few. Customers range in size from $25 million to $25 billion in annual revenue.

Maxxsure was founded in 2016 with the mission of developing the best-in-class cyber risk quantification and management solution that takes a truly holistic survey of all internal and external influencing factors over the cyber risk posture of an organization.

With Maxxsure, organizations have continuous line of sight into their cyber risk, allowing them to access up-to-date data to make adaptations to their cyber risk management strategies as their needs and environments change. The company provides a platform for executive management, leveraging proprietary technology that:

- *Identifies, measures, and scores an organization's cyber risks*
- *Uncovers hidden risks in a business model, including vendors/supply chain*
- *Illustrates how prepared/resilient an organization is against a cyber event*
- *Estimates potential financial loss of future events*

MAXXSURE

www.maxxsure.com

CORPORATE OFFICE:
4570 Westgrove Drive Suite 235
Addison, Texas 75001 USA

References Cited

(1) Cybersecurity Ventures Special Report: *Cyberwarfare in the C-Suite* by Steve Morgan, October 17, 2022.

(2) McKinsey & Company, *Cybersecurity Trends: Looking Over the Horizon*, March 10, 2022, by Jim Boehm, Charlie Lewis, Kathleen Li, Daniel Wallace, and Dennis Dias.

(3) "A C-suite united on cyber-ready futures," Findings from the 2023 Global Digital Trust Insights Survey, PwC

(4) Cost of a Data Breach Report "*2023 is the Year of Cyber Risk Quantification: CRQ is the hottest thing in cybersecurity right now,"* by John Chambers, Founder and CEO of JC2 Ventures. The article originally appeared in TechCrunch on November 7, 2022.

(5) Deloitte Perspectives: *Sharpening the Board's Role in Cyber Risk Oversight,* by Deborah DeHass, Vice Chair, Deloitte, and Ed Powers, Principal, Deloitte, January, 2023.

(6) Harvard Business Review - IT Security Management, *Is Your Board Prepared for New Cybersecurity Regulations?* By Dr. Keri Pearlson and Chris Hetner, November 11, 2022

(7) Gartner/Gartner IT Symposium 2021/ Sam Olyaei- *Gartner's 8 Cybersecurity Predictions for 2023-2025,* Feb 16, 2022, Krontech

(8) Harvard Business Review, Risk Management, *"The Cyber insurance Industry Has a Big Problem,"* by Tom Johansmeyer, January 11, 2021.

(9) Arthur Gallagher and Company, Cyber Liability Practice, *Cyber Risk Exposures and Solutions,* by Adam Cottini, Managing Director, Cyber Liability Practice, January, 2023.