Brought to you by Informa Tech

Cybersecurity Risks, Trends & Market Intelligence

Challenges and opportunities in the cyber ecosystem

Introduction

Cybersecurity is complex, yet organizations must be able to deal with security incidents and breaches to maintain continuous operations in today’s digitally dependent world.

Resilience is no easy feat. Enterprises face double-whammy ransomware, whereby threat actors not only lock your data but also threaten to expose it if you don't pay up. There's compliance, driven by governments and industry bodies to ensure that organizations are taking cybersecurity seriously. Chief Information Security Officers (CISOs) report no lack of appetite for continued innovation, so the security function must stay on its toes as evermore capabilities are made available to customers and citizens. Layer geopolitical issues on top and maintaining cyber-resilience becomes a dizzying array of challenges for CISOs and their teams – and the organization itself.

Black Hat Europe is a timely reminder of these important issues, presenting an opportunity for us to engage in conversation about the ongoing challenges. We hope that you find the excerpts of our research useful in understanding the current and future trends in cybersecurity and invite you to join the conversation.

Maxine Holt, Senior Director - Cybersecurity
Maxine.Holt@omdia.com

Our analysts at Black Hat Europe

Hollie Hennessy
Senior Analyst
IoT Cybersecurity

Maxine Holt
Senior Research Director
Cybersecurity

Eric Parizo
Managing Principal Analyst
Cybersecurity

Don Tait
Senior Analyst
Cybersecurity

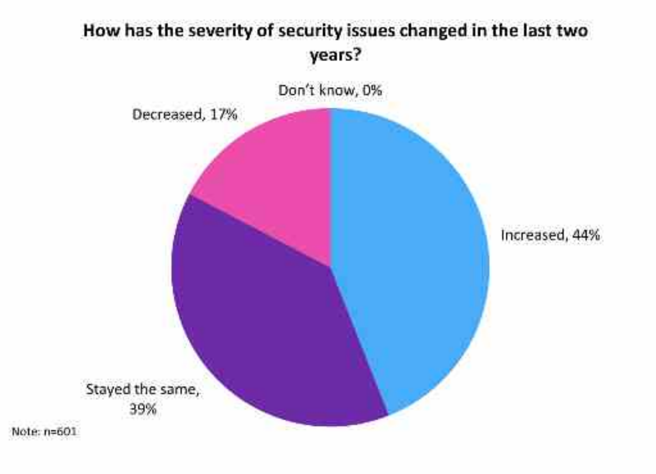
Rik Turner
Senior Principal Analyst
Cybersecurity

Brought to you by Informa Tech

Industry Insights from the Security Decision-Maker Survey

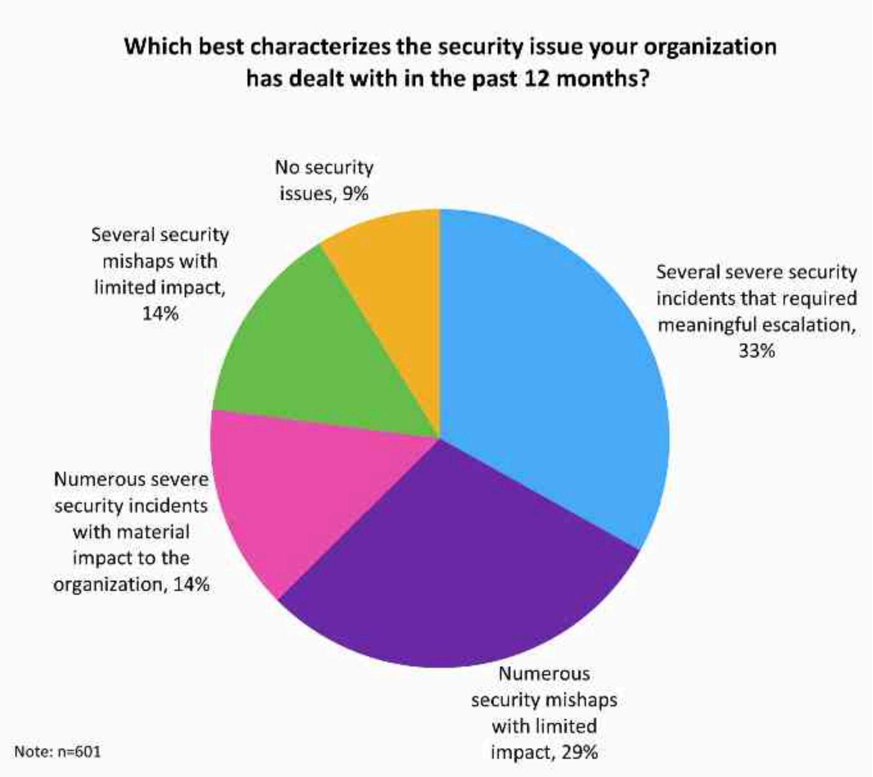
Omdia's security decision-maker survey 2022 shows that only 17% of organizations globally believe that the severity of security issues has decreased since 2020, leaving 83% stating that they have either stayed the same or increased.

The survey also asked about the level of security issues in the past year, and only 9% of organizations reported that they had no security issues, with a further 14% describing the issues as pretty minor. But this does leave over three-quarters of organizations with security issues ranging from multiple incidents with limited or material impact, through to the one-third of organizations with several severe security incidents.



Source: Omdia

Copyright © 2022



Source: Omdia

Copyright © 2022

Enterprises face significant challenges as they try to bring security issues under control. There is pressure from multiple directions to stay secure. Cyberattacks remain front and center, whether ransomware, supply chain attacks, business email compromise, negligent or accidental acts by employees, and so on, when it comes to security.

But there are other forces at play, so, intervention in the form of legislation or regulation by governments or industry bodies, to protect customers or citizens, or ensure that critical national infrastructure meets minimum standards to stay operational. Then we have innovation, and this applies to public and private sector organizations alike, always pushing for the latest capabilities to support customers and citizens. And last, but by no means least, is the need for resilience; what many organizations face today is a band-aid on security that frequently is not fit for purpose. Being able to provide continuous operations despite security incidents and breaches is crucially important for organizational resilience. Organizations must step up their game so that their digital first approach also applies to cybersecurity.

To request more information feel free to email:

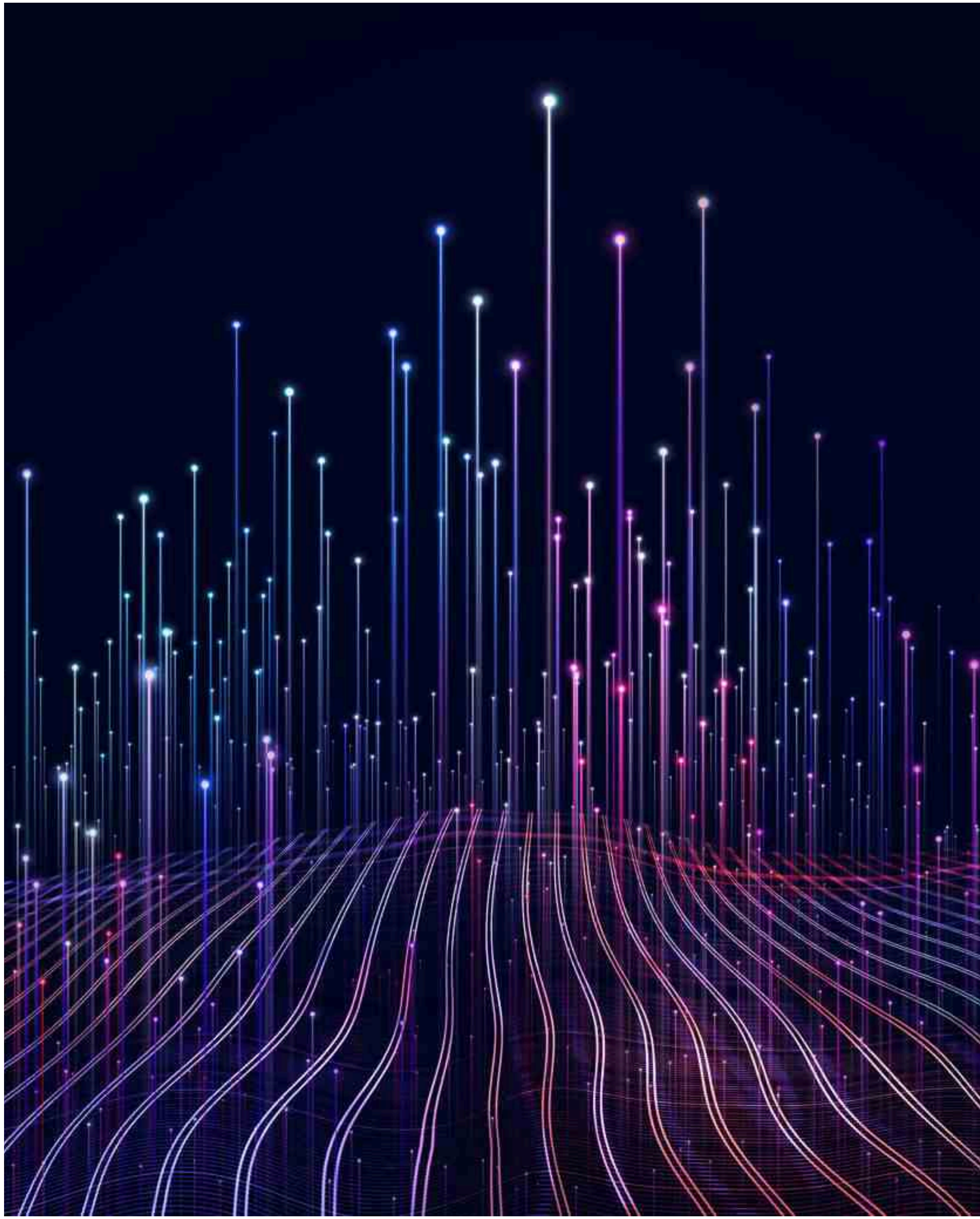
Maxine Holt, Senior Director - Cybersecurity
Maxine.Holt@omdia.com

Data Exposure: The Prevailing Breach Outcome 2019 -2021

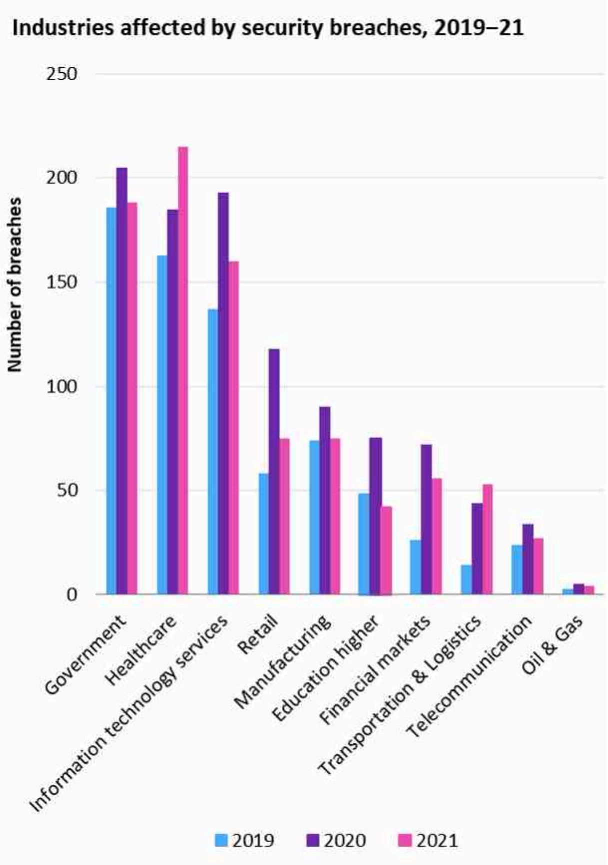
Omdia tracks reports (in English) on security breaches, highlighted in its Security Breaches Tracker, 2019-2021. Looking at the data from these three years, data exposure is the most prevalent breach outcome, standing at two-thirds (2,491 announcements) of the cumulative breach outcomes.

The sheer quantity of leaked records, personal information, and other sensitive data highlights the pervasive issue. System failure comprised 16.0% of the breach outcomes, followed by process failure (4.8%) and industrial espionage (4.4%).

Against the backdrop of the jump in cyberattacks, organizations show improved awareness of data management. Omdia's IT Enterprise Insights 2022 (a survey of around 5,000 respondents from 56 countries in 26 major industries) illustrates that the management of security, identity, and privacy is the leading IT trend for 19.6% of organizations. Even more promising are IT investment plans in the security technology category, again revealed through Omdia's IT Enterprise Insights 2022 survey; 34.6% of organizations have strategic investments planned for data security, including data loss prevention (DLP), encryption, tokenization, and privacy management, while 31.8% of organizations plan minor investment for data security.



Governments, healthcare, and IT industries were heavily affected



Source: Omdia

From the tracked breaches, the main industries affected from 2019 to 2021 include governments (15.4%), healthcare (15.0%), and IT services (13.0%). Across all industries, data exposure dominates the breach outcomes at 66.3%, followed by system failures (16.0%) and process failures (4.8%).

Government bodies, including state and local governments, and other agencies are some of the main targets of hackers. Omdia's Security Breaches Tracker documented 263 breaches across US government agencies from 2019 to 2021, including the Central Intelligence Agency (CIA), the US Census Bureau, the Department of Justice, and county- or city-level organizations.

The sheer amount of data housed by government agencies and its interdisciplinary nature are sufficient to attract hackers to access the goldmines of information. Government agencies that rely on contractors and third parties increase the risks of cyberattacks. Moreover, state and local governments that are less funded than federal institutions may have a severe lack of bandwidth and resources for adequate protection against large-scale, malicious attacks.

To request more information feel free to email:

Maxine Holt, Senior Director - Cybersecurity
Maxine.Holt@omdia.com

The Growth of IoT Devices Increases the Attack Surface

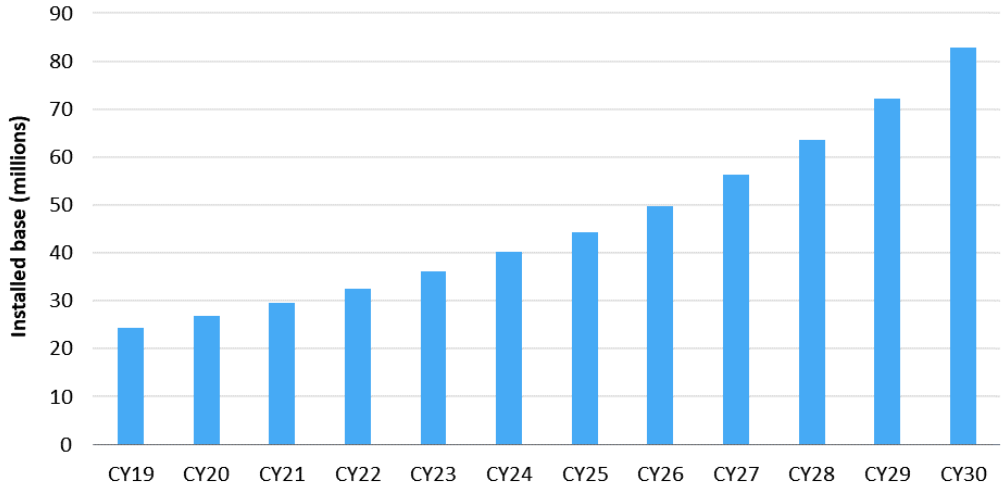
Attack surfaces are likely to widen as organizations across a range of industries adopt IoT technology to empower new business models. By 2030, Omdia expects the total IoT device installed base in a range of applications to reach 82.6 billion.

As indicated in Omdia's 2022 Trends to Watch: IoT Cybersecurity report, IoT devices are insecure by design primarily because of limitations in computing power, lack of comprehension, and preferences for usability and low costs over security. The lack of proper policies, regulators, a coherent security standard, and a unified approach further exacerbates challenges in IoT cybersecurity.

In addition, the interconnected nature of IoT—where physical devices are connected to the internet and other connected devices—and its ability to collect and share data creates growing attack surfaces for threat actors. As more information and data is passed back and forth through numerous connected devices, this points to exploitable vulnerabilities and doorways that lead to security breaches.

Cloud technology and further developments in global smart city initiatives, which feature IoT connectivity in major functions of cities including transportation, energy efficiency, physical infrastructure, safety, and healthcare, will highlight the prevalence of IoT in the coming years and contribute to more attacks on connected infrastructure.

Total IoT device installed base, 2019–30



Source: Omdia

Copyright © 2022

To request more information feel free to email:

Hollie Hennessy, Senior Analyst - Cybersecurity
Hollie.Hennessy@omdia.com

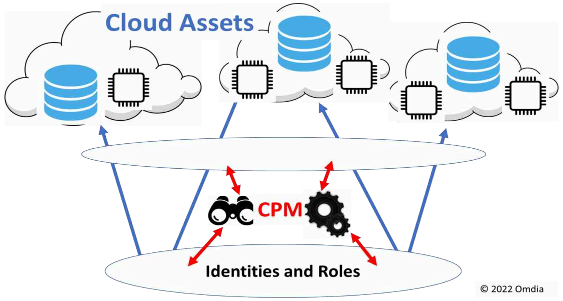
Brought to you by Informa Tech

Applying Zero Trust to Enable Cloud Permissions Management

Cloud adoption continues apace around the world, driven by the digital transformation that has itself been turbocharged by the coronavirus pandemic.

As application infrastructures move to the cloud, however, the need to secure corporate assets residing in cloud environments has become an ever-increasing requirement. There is growing interest in preemptive approaches that adopt an a priori stance to cloud security, reducing the attack surface before exploits can even take place.

The mindset behind such attitudes is nowadays referred to as "zero trust." Zero trust is a mindset or, if you prefer, a philosophical stance on security, which can be summed up as "never trust, always verify"—to which Omdia nowadays adds a third dimension, "...and continually monitor." An example of zero-trust technology in cloud security is cloud permissions management (CPM), shown in the diagram.



Source: Omdia

CPM begins by drawing up a full inventory of the extant permissions within an organization's cloud estate. Once that process is complete a CPM platform carries out an analysis of all the permissions listed against the various identities to determine which ones are excessive or simply surplus to requirements. It then makes recommendations for how the permissions estate can be curtailed, with individual access rights being reined in or removed altogether. Some CPM platforms can also go further, actually performing the remedial action they have recommended in an automated fashion if the customer is happy to enable that feature.

Omdia does not believe that CPM will remain a standalone capability, taken to market by vendors dedicated exclusively to its further development, for very long. It makes sense for CPM to be part of a broader portfolio of security capabilities, whether specifically for the cloud or for hybrid environments spanning both the cloud and on-premises infrastructure.

To request more information feel free to email:

Rik Turner, Senior Principal Analyst
Rik.Turner@omdia.com

Brought to you by Informa Tech

Passwordsless Authentication Gaining Momentum

The world is rapidly moving away from proprietary, monolithic authentication methods that rely on shared secrets to standards-based, passwordless solutions that prioritize security and usability. Multi-factor authentication (MFA) is already seen as the default requirement for basic security, so now the issue becomes how to evolve the various factors to improve it further. Passwords clearly must go; the challenge is becoming how to make biometrics both secure and affordable.

There is no reason why the password cannot be replaced by something such as biometric information (e.g., a thumbprint or scanned iris). This is particularly the case if the biometric data can be stored securely on a mobile phone, so the user can authenticate locally to the phone and then the phone can authenticate, without using the biometric data, to a backend server across the network.

Fingerprint and facial recognition
Gestures
Identifiers
Cellular handset
Behavioral patterns
Cryptographic keys
Face ID
Geolocation
Hardware token
FIDO2
~~Username and password~~
OPT token
WC3
Better UX
Windows Hello
WebAuthn

Getting rid of passwords has been the holy grail for many organizations and individuals over the past 30 years. 2022 has heralded the start of passwordless authentication becoming more established and mainstream. If traditional MFA is a password with one or more authentication factors, passwordless MFA is best described as two or more authentication factors without a password.

Passwordless authentication eliminates the reliance on passwords and delivers a host of business benefits, including better user experience, reduced IT time and costs, and a stronger security posture. However, it is not an end in itself. A sound authentication system should build upon a long-term vision to foster security, privacy, sustainability, user experience, scalability, and inclusiveness.

For passwordless to become a reality, all stakeholders need to work together: technology platform providers, hardware and software vendors, standards organizations, and enterprises, to name just a few.

To request more information feel free to email:

Don Tait, Senior Analyst - Cybersecurity
Don.Tait@omdia.com

Thank you for reading

Cybersecurity Risks, Trends & Market Intelligence