Enterprise evolution and the role of cybersecurity

OMDIA

Brought to you by Informa Tech

Introduction

As cyber risk continues to gather pace, cyber risk investment on the other hand, has slowed down amidst global economic changes and uncertainty.

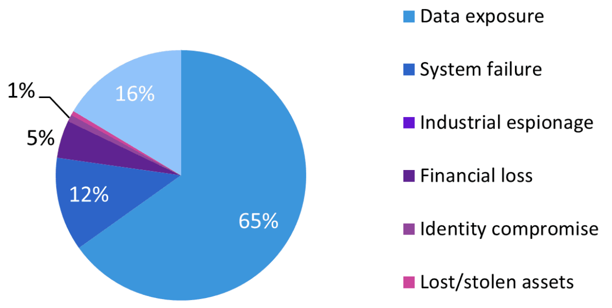
As cyber risk continues to gather pace, cyber risk investment on the other hand, has slowed down amidst global economic changes and uncertainty.

Since the last publication of the World Economic Forum's (WEF) 2022 Global Risks in January 2022, significant global events have taken place. Russia's invasion of Ukraine and the consequential impact on food and energy supply has led to a cost-of-living crisis that has echoed across the globe. Extreme weather events are becoming common for more and more people. These rapid changes form the backdrop of 2023 and while there is no single dominating crisis currently facing the world, there are—and will continue to be—constant crises that organizations, governments, and countries must navigate. The WEF's 2023 Global Risks Report (published January 2023) has identified attacks on critical national infrastructure and widespread cybercrime and cyber insecurity as major risks to remain vigilant for throughout the next 10 years.

Cybercrime is an everyday reality. As just one example, ransomware continues to be a scourge on society and organizations, but the potential opportunities and yields are so great that it is here to stay. Phishing, crashing websites, and identity theft are just some further examples of cybercrime that will continue.

Omdia's Security Breaches Tracker has consistently shown that data exposure is the leading outcome of security breaches, accounting for around two-thirds of breaches in 2022 (see Figure X).

Figure X: Share of breaches by outcome, 2022



This approximate two-thirds number has been consistent since 2019 (68% in 2021, 67% in 2020, and 64% in 2019). The tracker also analyzes the share of breaches by industry (or vertical), and healthcare was the biggest sector to be affected by security breaches in 2022, followed by the government sector. The healthcare and governmental sectors have interchanged the "top spot" over the same three-year period for data exposure. It is fair to say that data is poorly protected today, and that government and healthcare are huge targets for data because of the extent of personally identifiable information (PII) that they hold.

Throughout this e-book our experts explore data and share insights on the cybersecurity considerations for enterprises as they continue to grow.

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

Security budgets amidst the cost-of-living crisis

Although cybersecurity has a high profile in many organizations, it rarely follows that the budget matches the profile. Furthermore, security budgets are not often in the sole control of the Chief Information Security Officer (CISO), instead often at least in part with the Chief Information Officer (CIO) or other functions.

Omdia's cybersecurity decision-maker survey of 2022 asked what percentage of an organization's security budget is allocated to emergency incident response, and just over two-fifths of organizations allocate less than **10%** of their security budget to this area. This indicates one of two things; either that they are reasonably confident in their security controls, or that they simply don't have sufficient budget for emergency incident response. The reality is that it is likely a mixture of the two, given that only one-third of organizations are "extremely confident" in their security controls. We also know that around **58%** of organizations use external providers for emergency incident response. The focus on security isn't going away but dealing with incidents as and when they happen will impact those organizations without allocated budget.

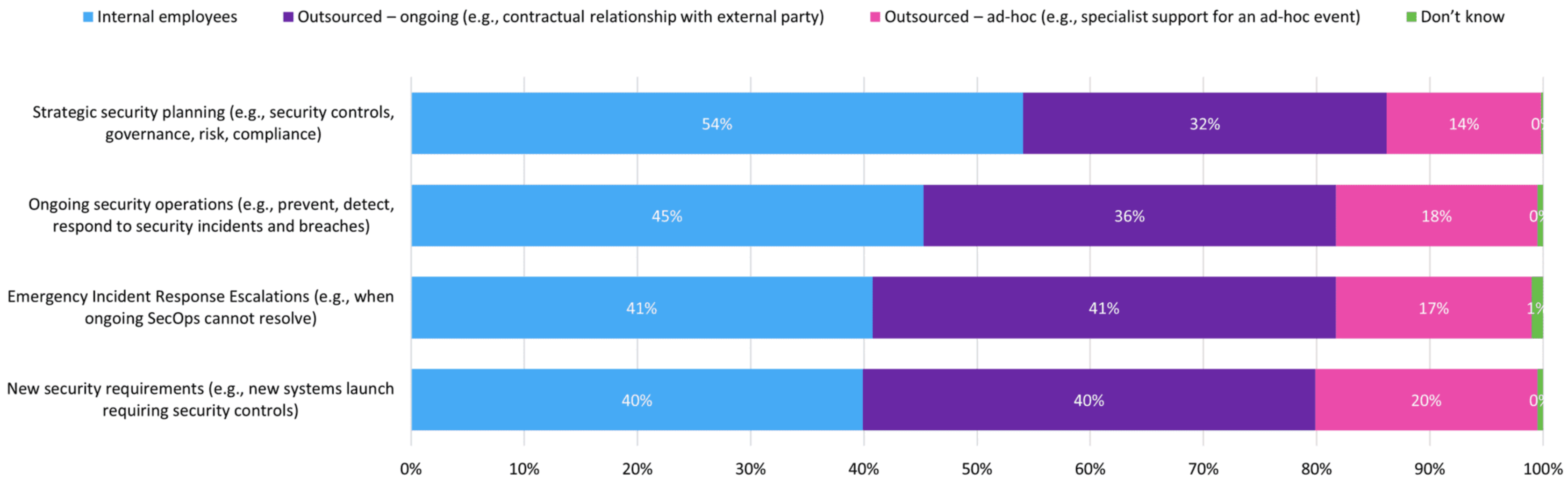
It is interesting to note that when the cybersecurity decision-maker survey took place, just **20%** of organizations expected their security budget to increase by over **15%**. A further **50%** anticipated a moderate increase of up to **15%** – when taking inflation into consideration this could become a very moderate increase – leaving **30%** with an anticipated decrease in their security budgets. The 2023 cybersecurity decision-maker survey asks the same question this year, and Omdia anticipates that there will be fewer organizations with an anticipated increase, with most budgets staying static or reducing.

One of the ways in which organizations look to address their security challenges is by augmenting their workforce with managed security services. This same survey noted that outsourcing, whether an ongoing relationship with a provider or ad hoc according to need, is widely used (see Figure X on the following page).

The security workforce challenges mean that many organizations struggle to fill vacancies in a timely manner, and managed security services is one way of filling the gap, whether on a temporary or indeed more permanent basis. Furthermore, the cybersecurity market moves quickly, and it can be challenging to upskill inhouse; managed security service providers help here.

Ultimately, attention on security will not wane but CISOs and their teams must find different ways of making their budgets go further. We've heard it all before but the mantra is: "more with less"

Figure X: Internal and external resourcing



Notes: n=601
Source: Omdia

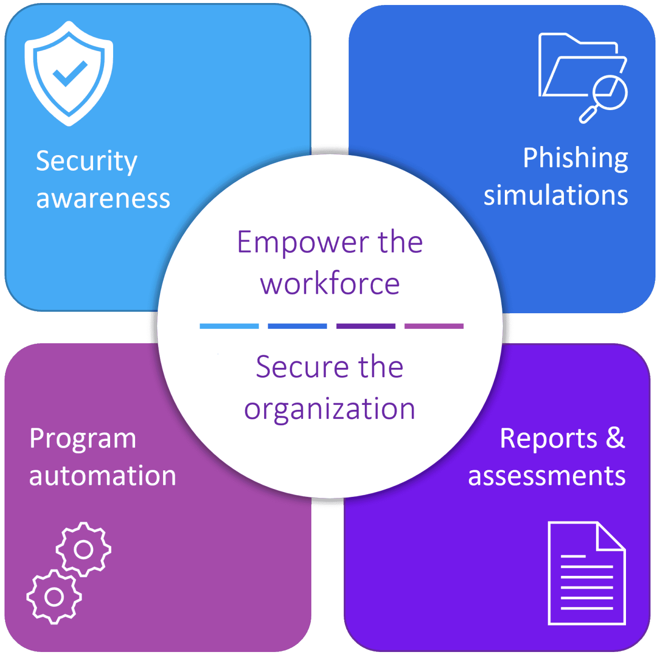
© 2023 Omdia

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

Brought to you by Informa Tech

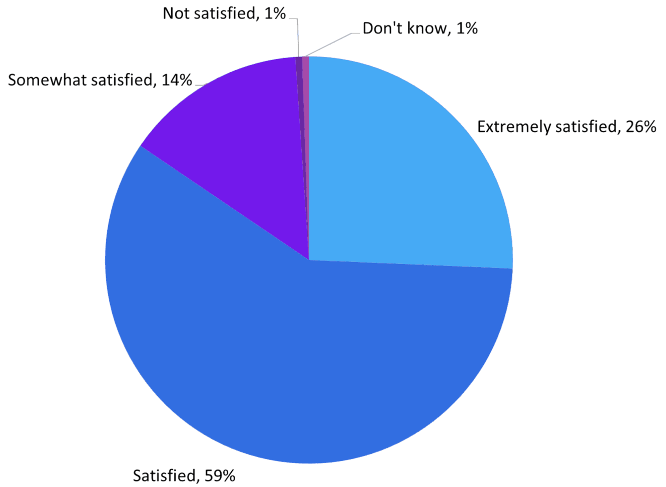
Embedding cybersecurity awareness into organizational DNA

All too often at Omdia we hear the comment “people are the weakest link” when it comes to cybersecurity. Instead, this should be rephrased to those “untrained and uneducated in cyber risk are the weakest link”.



Cybersecurity awareness training (CAT) is essential to ensure that those using an organization’s systems are trained and educated into being secure as a way of operating. Omdia’s cybersecurity decision-maker survey found that just over one-quarter of organizations are extremely satisfied with their current CAT programs (see Figure X)

Figure X: How satisfied are you with the quality and results from your cybersecurity awareness training program(s)?



Note: n=187
Source: Omdia

© 2023 Omdia

This is a good number, especially when added to the 59% reporting themselves as satisfied, yet security incidents and breaches relating to people continue to happen. People click on links. People open emails. People do lots of things that contribute to operating insecurely.

Cyber awareness training (CAT) as a discrete activity tends to dissolve into the employee’s daily workflows. At Omdia we expect that CAT will increasingly disappear as a discrete activity involving the dedication of 45 minutes of an hour to an online course. The efficacy of traditional CAT is at best only high for a point in time and soon wanes once the course has been completed. The new thinking on CAT is to incorporate it into regular work activities, making it less intrusive and more user friendly as a result. Organizations will test whether this less invasive approach to CAT is more effective in their particular workforce, perhaps by running a test with one set of employees while another set continues on a traditional training platform.

As such, CAT moves from being a point-in-time intervention with someone who has clicked on a link in a simulated phishing email, with a refresh every six months or once a year, and becomes a continuous process of checking on how employees are operating and interacting with the organization’s systems.

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

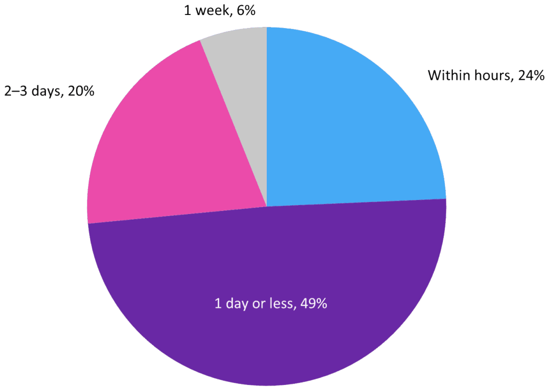
Brought to you by Informa Tech

Mitigating and responding to an organizational PII security breach

Security incidents and breaches continue to hit the headlines. Far too often, there are examples of personally identifiable information (PII) being exposed, whether through lax security controls or the subject of a targeted and sophisticated attack.

The focus for Security Operations (SecOps) functions is generally on reducing the mean time to detection (MTTD) and mean time to response (MTTR) for security incidents and breaches. Most organizations will aim for minutes or hours to resolve such incidents – currently only achieved by fewer than one-quarter of survey respondents.

How quickly can your organization respond to, and successfully resolve "high" priority security events?



Note: n=181. Percentages are rounded to the nearest whole number and do not always add up to 100%
Source: Omdia

© 2023 Omdia

Considering PII breaches in particular, security focuses on protecting the confidentiality, integrity, and availability of information—frequently referred to as the CIA triumvirate. The confidentiality portion focuses on data privacy, and this has been a key legal requirement for enterprises for decades. However, preventing the disclosure of PII is not always successful. On one end of the scale, an organization might be subject to a highly sophisticated and targeted attack to steal specific information; on the other end of the scale, an organization might employ few or no security controls to provide data protection. The outcome is the same across this scale: PII that should have remained private has been exposed.

Governments around the globe have implemented increasingly stringent legislation designed to protect the individual when it comes to maintaining data privacy. These regulations can vary quite significantly region by region. Organizations operating in multiple locations can sometimes have conflicting regulations to deal with, creating challenges when demonstrating compliance in the event of a data privacy incident or breach.

Incident response playbooks are crucial, particularly when some legislation requires notification within hours of breach discovery. Being ready and prepared to respond with a set of predefined processes and workflows in the event of a breach supports compliance with requirements in the region(s) where the legislation applies. Furthermore, a centralized source of regulations, playbooks incorporating as much automation as possible, and case management capabilities help accelerate response and facilitate coordination across the different functions involved, such as HR, Legal, and Marketing (among others).

This market is not going away anytime soon—data privacy requirements are only going to increase. Organizations must be able to manage security incidents and breaches quickly and effectively. Complying with data privacy regulations can help mitigate the impact of a breach, including any short- or longer-term damage to organizational reputation.

Eric Parizo, Managing Principal Analyst
Eric.Parizo@omdia.com

Brought to you by Informa Tech

Evolving technologies and cybersecurity risks: Artificial intelligence

Machine-based intelligence, known more commonly as artificial intelligence (AI), is in the process of remaking cybersecurity, and companies are leaning into its use for ever more purposes.

A growing skepticism in the halls of government about the benevolence of AI indicates that limits may be on the horizon for the most aggressive application of the technology. Many of the ideas around potential limits or guidelines can be found in 2022's "Blueprint for an AI Bill of Rights" released in October 2022 by the White House. The major concepts contained in the blueprint center on AI-based systems designed with privacy, appropriate use, and data security as inherent qualities, and system users who are kept fully informed of an AI-based system's presence, qualities, and limits.

In this context, "AI" is used as a term that refers to artificial intelligence, machine-based intelligence, deep learning, and all of the terms used for various forms of advanced algorithmic machine learning. The subtle but notable differences between these technologies is acknowledged, but they are being considered together.

Whether the topic is analysis or automation, cybersecurity is now informed by AI: its various forms play growing roles in the software and services of cybersecurity. Perhaps because of AI's ubiquity in cybersecurity, questions about the roles it should play, and how it will play those roles, are being asked by many inside and outside the industry.

Cybersecurity teams can stay ahead of potential laws, regulations, and industry guidelines by focusing on three words as they apply to AI. Intention, responsibility, and transparency will be key to creating systems that won't have to be walked back under future regulatory regimes.

Intention: It is important to plan AI-based systems so that their design, development, training, and use are all managed in order to meet a specific need. Limiting the system (and the data required to feed it) to fit a purpose will help avoid gathering more user information than is required—information that then has to be protected from internal and external misuse.

Responsibility: Organizations must be responsible for the systems they build and the data they use and store. That means building security and privacy into the system (rather than adding it after a breach) and ensuring that there are policies, procedures, and responsible employees in place to protect those who use the system. It also means taking care to test the system before deployment to guard against unintentional bias skewing results in ways that place demographic or other groups at an algorithmic disadvantage.

Transparency: Legitimate users should understand that their actions are being vetted by AI, that their access is controlled by an AI, and that their security is insured by an AI-based system. They should have a clearly stated way to communicate with a human in the case of unanticipated results, and they should know what data is being gathered about them and how the gathering organization is securing personal information used by the AI. The AI-using organization doesn't have to give away all their security secrets, but they do have to make sure that the humans using their systems are willing participants in an artificial intelligence world.

Curtis Franklin, Senior Analyst, Security Operations, Enterprise Security Management
Curtis.Franklin@omdia.com

About Omdia

stop error screen, restart you
follow these steps:
space. If a driver is identified
disable the driver or check with the manufacturer for
Try changing video adapters.
ware vendor for any BIOS updates. Disable BIOS memory
caching or shadowing. If you need to use Safe Mode to
components, restart your computer, press F8 to sel
options, and then select Safe Mode.
(0XFFFFFFFFC0000005, 0XFFFFF8800536CA9,
002590E30)

About Omdia

Omdia, part of Informa Tech, is a technology research and advisory group. Our deep knowledge of technology markets combined with our actionable insights empower organizations to make smart growth decisions.

Assess

Assess opportunities and trends drawing on our deep knowledge of technology markets.

Advance

Advance your business strategy; reduce cost and risk using our actionable data and insights.

Amplify

Amplify your presence by leveraging our access to audiences, events and media in the tech ecosystem.

From concept and product development, to go-to-market and sales effectiveness, we can help you grow your business. We do this through our syndicated research, consulting services, as well as our ask an analyst offering.

Syndicated Research

Our leading forecasting and insights research covers the full spectrum of the technology industry, providing access to over 200 million data points, with more than 250 forecasts and over 3,000 reports published annually.

Consulting

Our consulting team acts as an extension of your team, partnering with you on custom projects, from market sizing to evaluating the competitive landscape and advising on go-to-market strategies.

Ask an Analyst

Leverage unique access to market leading analysts and profit from their deep industry expertise during tailored Ask An Analyst sessions included in your subscription.

Further information

Website

Contact us form

Ask An Analyst

Brought to you by Informa Tech

Thank you for reading

The role of cybersecurity in the evolution of enterprises