ecosystm

ECOSYSTM PREDICTS

The Top 5 Trends for Cybersecurity & Compliance in 2022

PUBLISHED

November 2021

Andrew Milroy
Principal Advisor,
Cybersecurity, Cloud,
IT services & Digital
Transformation

Claus Mortensen
Principal Advisor,
Digital Transformation,
Cloud Computing

Introduction

Cyber operations become more complex with distributed company assets due to the hybrid work model; the need to revamp supply chains; and constantly monitor business continuity measures. And of course, 2021 has shown us that hackers are getting smarter and more vicious. Attacks now often originate from what appears to be trusted devices, people, applications – that reside inside the network. This will drive organisations to continue to focus on cybersecurity (Figure 1); and tech providers to develop security by design in 2022.

FIGURE 1: ORGANISATIONS WILL CONTINUE TO FOCUS ON CYBERSECURITY

62%
Concerned about phishing and malware

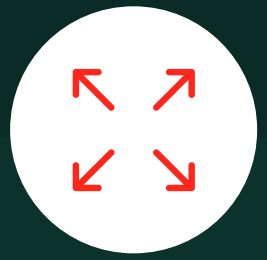
70%
Think a data breach is inevitable

74%
Invested more on cyber solutions in 2021 over 2020

67%
Have Security & Resiliency as the key focus in 2022

Source: Ecosystm, 2021

Ecosystm Rates the Cybersecurity & Compliance Predicts for 2021



There will be Further Expansion of M&A Activities Through 2021 and Beyond

This has held true. 2021 was a boom year for M&A activity overall, and Cybersecurity was not an exception. We expect the trend to continue in 2022.

After a Year of Pandemic Leniency, Regulators will Get Stricter in 2021

While regulators may not have been quite as active in 2021 as we expected, we did see more activity. As for new regulation, this has mostly been pushed to 2022.

The Zero Trust Model Will Gain Momentum

Zero Trust has been a major focus point, with most vendors pushing their solutions to the market. However, there is still some hesitancy in some sectors.

The Endpoint Will be the Weakest Link

Endpoints have been the focus of many cyber attacks in 2021. The attacks from IoT and 5G endpoints have not yet been significant though.

Hackers Will Turn the Table on AI Security

We were probably a year early on this one. Deepfake attacks using voice calls have reportedly been taking place, but large-scale use of AI will probably wait until 2022 or 2023!

#1 Rush to the Cloud Will Drive a Greater Focus on Configuration Management

The rapid deployment of workloads in the cloud is often a major burden for security teams. Growing 'operational sprawl' adds to security complexity and often leads to misconfigured clouds.

For example, IaaS solutions typically require extensive configuration to make sure that they work properly. Often, the need to configure IaaS solutions in line with a company's desired security posture is overlooked, potentially leaving data exposed to the public. Incorrect configuration can result in storage offerings (such as AWS S3) being exposed. Access to this data can easily be indiscriminately granted to anyone who tries to access it, which can have a devastating impact.

Repairing misconfigurations is an essential part of data leakage prevention and is critical to ensuring that cybersecurity postures are effectively managed. Expect to see greater focus on cloud configuration management in 2022.

The rush to the cloud has often made cloud security a secondary issue. Misconfigurations are alarmingly common. In 2022, configuration management will be central to cloud security.

Andrew Milroy
PRINCIPAL ADVISOR, CYBERSECURITY, CLOUD, IT SERVICES & DIGITAL TRANSFORMATION

#2 Major Cloud Providers Will Struggle to Maintain Their "More Secure" Status

One of the initial reasons for most organisations to hold back on cloud adoption was the perceived lack of security. As the years have gone by however, major cloud providers have largely succeeded with their argument that only they, as large international service providers, had the scale and range to achieve the high levels of security needed in today's environment. There have been issues in the past, but most could be attributed to "user error" as cloud customers have misconfigured part of their networks.

But the cloud architecture of major cloud service providers have been known to be a source of security breaches among their customers and we don't expect the "more secure" label to last.

As most organisations now rely on large cloud providers for a major part of their systems and as more and more Operational Technology (OT) is getting linked to them as well, we expect leading cloud service providers to become a main target for hacker groups. And we fear that they may succeed in 2022, forcing cloud providers to drastically beef up their security paradigms.

"Trust" is a fickle selling point, and a major breach could be a public relations disaster for not just the cloud provider that was breached, but for all major cloud service providers. Their Sales and Marketing teams may have to work overtime to re-establish previous levels of trust in 2022.

Claus Mortensen
PRINCIPAL ADVISOR,
DX & CLOUD

#3 DevSecOps Drives Shift to Policy-As-Code

As companies start to embrace DevSecOps, developers will act as policy enforcers by building policy into code.

Security by design will become more common, as security programs align with DevOps to provide the automation required to secure complex technology environments. Developers will start to see baking security into code, not as an inconvenience, but as a critical part of creating new applications rapidly.

Not all policies can be implemented as code. In 2022, expect to see access, governance and configuration policies increasingly being implemented as code.

2022 will be the year when we witness companies building security into everything they do. Developers will become more comfortable with baking security into code.

Andrew Milroy
PRINCIPAL ADVISOR, CYBERSECURITY, CLOUD, IT SERVICES & DIGITAL TRANSFORMATION

#4 SASE Will Accelerate Migration from Legacy Perimeter-Based Approach

The traditional network infrastructure model of centralised corporate data centres secured by on-premises network perimeters, does not work today. Data that once resided in data centres is increasingly found in the cloud, on SaaS applications, and on endpoints.

Frequently, security controls are not designed for the dynamic, distributed, and virtual nature of cloud environments, and widely dispersed remote working.

Companies require the ability to deliver an integrated set of network and security services in a consistent way — enabling digital transformation, cloud migration, edge computing and remote working.

These requirements can be addressed by secure access service edge (SASE) strategies. Expect to see a wider adoption of SASE strategies in 2022.

In 2022, companies will start to understand what SASE means and its importance as a strategy, as they embrace the cloud, the edge, and remote working.

Andrew Milroy

PRINCIPAL ADVISOR, CYBERSECURITY, CLOUD, IT SERVICES & DIGITAL TRANSFORMATION

#5 Cyber Attacks Will Focus on Supply Chains

Supply chains have been stretched to their limits and beyond, in the last couple of years – mostly due to COVID-19, but other events have factored in as well. This has made it more obvious how reliant society and vendors are on their supply chains. If one key component is missing, whole production lines may experience long delays (as we have seen with the current chip shortage).

The Kaseya and SolarWinds incidents in 2021 showed us how a breach of one part of a widely used system can compromise many. Attacking a relatively weak link of a larger supply chain can have far-reaching impact – well the one link that was compromised. This in turn, can multiply the number of organisations a hacker group can extort from, with one targeted attack. They will not be blind to this opportunity, and we expect large supply chains to be scrutinised and increasingly attacked in 2022 and beyond.

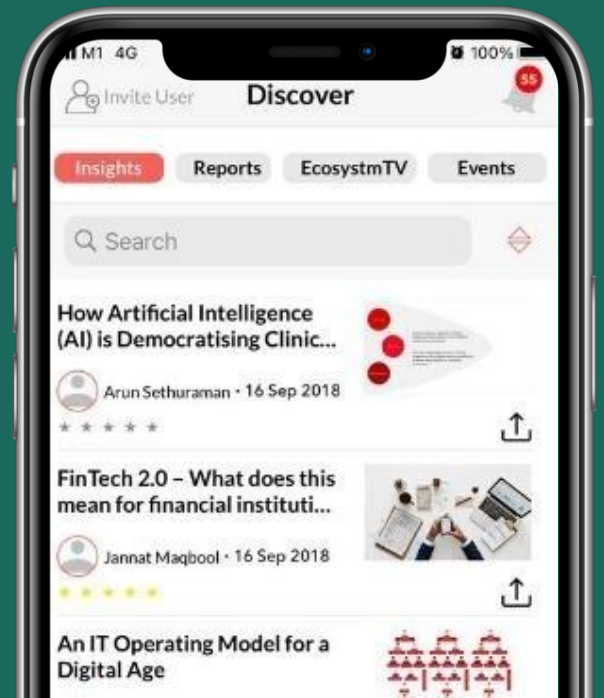
Hackers will always look for the weakest link. By targeting major or even global supply chains, they may find the weakest link affecting thousands or organisations. With one single attack, hackers can drastically increase the number of companies they can extort money from.

Claus Mortensen
PRINCIPAL ADVISOR,
DX & CLOUD

ecosystm

Engage our Analysts

For more information, visit:
www.ecosystm360.com
info@ecosystm360.com



Alex Woerndle
Principal Advisor,
Cyber Security

Andrew Milroy
Principal Advisor,
Cybersecurity & Digital Strategies

Carl Woerndle
Principal Advisor,
Cybersecurity

Claus Mortensen
Principal Advisor,
Digital Transformation,
Cloud Computing