ecosystm

ECOSYSTM PREDICTS

The Top 5 Trends for Cybersecurity & Compliance in 2023

PUBLISHED
December 2022

Alan Hesketh
Principal Advisor,
CIO Advisory & Digital Strategy

Alea Fairchild
Principal Advisor,
Infrastructure & Cloud Enablement

Andrew Milroy
Principal Advisor,
Cybersecurity & Digital Strategies

Sash Mukherjee
VP Content & Principal Analyst,
Industry Research

Going Beyond a Checklist

With organisations facing an infrastructure, application, and end-point sprawl, the attack surface continues to grow; as do the number of malicious attacks. Cyber breaches are also becoming exceedingly real for consumers, as they see breaches and leaks in brands and services they interact with regularly. 2023 will see CISOs take charge of their cyber environment – going beyond a checklist.

BIGGEST CHALLENGES CISOs WILL TRY TO MITIGATE IN 2023

42%
Compliance

36%
Low employee & stakeholder awareness

36%
Managing 3rd party risk

36%
Assessing cyber risk and posture

Source: Ecosystm Digital Enterprise Study, 2022

Ecosystm analysts present the top 5 trends for Cybersecurity & Compliance for 2023

#1 An Escalating Cybercrime Flood Will Drive Proactive Protection

A flood is coming, and many companies are not preparing sandbags to protect their assets from cybercriminals. Flood water gets into the smallest cracks.

Cybersecurity threats to an organisation are multiplying exponentially as bad actors access exploits as a service, making it possible for relatively unskilled people to benefit from cybercrime. Experienced and skilled threat actors are developing sophisticated tools, using AI to improve their success rate.

Organisations need to conserve resources in our challenging economic environment. Still, the escalating external threats mean reducing or just maintaining the current spending will increase the risk of a successful attack. Defence improvements will continue to protect an organisation's assets relative to their risks.

Successful flood defence comes from communities working together! Even in the current economic context, tech buyers must increase their investment in defences to stay ahead – don't't skimp on the sandbags.

Alan Hesketh
Principal Advisor,
CIO Advisory & Digital Strategy

#2 Incident Detection & Response Will Be the Main Focus

Widely publicised attacks in 2022 have shown that it has taken far too long to detect incidents, and responses have been slow and often inadequate. In 2023, organisations will assume that breaches will occur and focus on controls that allow them to detect and respond to incidents as quickly as possible.

As ransomware kits become cheaper and more readily available, organisations will need to deploy defence-in-depth to limit the impact of ransomware attacks. Attackers will inevitably penetrate company systems and networks, but layer upon layer of defence can make it impossible for the attackers to achieve their objectives.

Organisations will gradually develop a cybersecurity posture which allows continuous monitoring of internal assets, combined with the ability to adapt to changing threat and regulatory environments. Expect widespread use of automation and AI. Security orchestration, automation, and response (SOAR) will continue to grow in importance as security operations centres (SOCs) struggle to handle rapidly increasing workloads.

Defences must include immutable backups which should prevent a ransomware attack from interrupting or ceasing business operations, and the right mix of data masking techniques which will make any stolen data useless for attackers.

Andrew Milroy
Principal Advisor,
Cybersecurity & Digital Strategies

#3 Organisations Will Choose Visibility Over More Cyber Tools

Small and medium enterprises have always struggled to fund their cyber investments and appoint the right resources. This leads to a perception that enterprises are better-equipped to handle cyber risks. Recent CISO interactions show that this is not entirely correct. While some CISOs acknowledge that they get more budget for cyber tools and applications each time there is a high-profile breach in their country or industry, most say they simply do not have full visibility over all the cyber tools and measures they have in place to protect the organisations' IT and data environments.

Ecosystm research finds that on an average an enterprise uses 51 cyber tools that they are responsible for managing. CISOs talk about challenges such as finding, assessing and deploying, and maintaining the right tools; ensuring that the security tools are aligned to policies and processes; and reacting to too many false positives across multiple tools.

Organisations that have made significant cyber investments in the last few years will now invest in building a single pane of glass view of their cyber tools and applications. Many will find gaps in their cyber measures that will need to be filled urgently.

Sash Mukherjee

VP Content & Principal Analyst,
Industry Research

#4 Regulations Will Increase the Risk of Collecting & Storing Data

Questions are being asked about the need to collect and store so much PII. In many Asia Pacific jurisdictions, data is held for much longer than is necessary. The risk of a breach is often outweighed by the costs of cybersecurity modernisation. Recent attacks have changed risk calculations and governments are seeking ways to ensure that organisations place even more focus on protecting data. For example, the Australia Government has already made an amendment to privacy legislation, increasing penalties for serious or repeated breaches. Expect regulations in the region to be further tightened and penalties for weak data protection to be increased. This will increase the risk of collecting and storing data. Companies will collect less PII and ensure that there are time limits on data storage to reduce risk. It will also encourage organisations to modernise their cybersecurity postures.

Businesses will see the need to step back, assess their risks and current controls, identify the gaps, and put people and processes in place that can implement an adaptable posture that aligns with the new distributed technology environments.

> **Cybersecurity technology investments might come after a desired set of cybersecurity policies and processes have been determined.**

Andrew Milroy
Principal Advisor,
Cybersecurity & Digital Strategies

#5 Cyber Risk Will Include a Focus on Enterprise Operational Resilience

Enterprise downtime is more expensive than ever, which could include legal costs or financial penalties. Cybersecurity is critical in maintaining business continuity, particularly availability and up time with reputational and regulatory risk – all of which are key concerns for the Board, owner, and shareholder.

Investments in data velocity will be paramount, with a focus on 5G, edge, and cloud infrastructure and services to keep data moving. Enterprise operational resiliency is a combination of stable business operations, documented and assessed security risks, efficient workflows, and a cooperative and engaged employee base. Stabilising employee working conditions will be the focus in 2023 including effective hybrid working strategies supported by the right workflows and processes – with an eye on operational resilience.

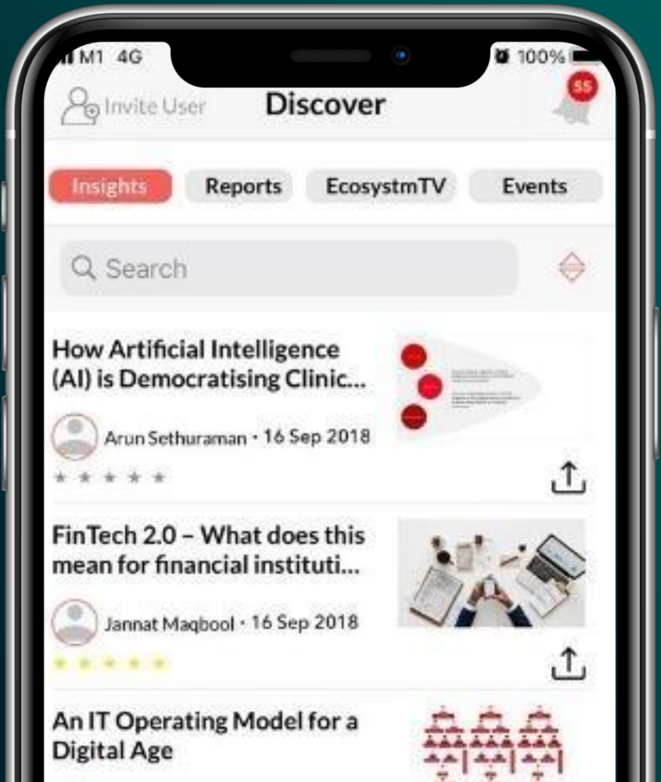
Managing cyber risk will become critical in 2023 and the CISO will become the ultimate 'risk officer' – at par with the CFO.

Alea Fairchild
Principal Advisor,
Infrastructure & Cloud Enablement

ecosystm

Engage Our Analysts

info@ecosystm360.com
www.ecosystm360.com



Discover

Insights Reports EcosystmTV Events

Search

How Artificial Intelligence (AI) is Democratising Clinic...
Arun Sethuraman · 16 Sep 2018

FinTech 2.0 – What does this mean for financial instituti...
Jannat Maqbool · 16 Sep 2018

An IT Operating Model for a Digital Age

Alan Hesketh
Principal Advisor,
CIO Advisory & Digital Strategy

Dr. Alea Fairchild
Principal Advisor,
Infrastructure & Cloud Enablement

Andrew Milroy
Principal Advisor,
Cybersecurity & Digital Strategies

Alex Woerndle
Principal Advisor,
Cybersecurity

Carl Woerndle
Principal Advisor,
Cybersecurity

Claus Mortensen
Principal Analyst,
Customer Experience & Customer Voice

Darian Bird
Principal Advisor,
Cloud, IT Services, Telecommunications

Peter Carr
Principal Advisor,
Strategy & Technology Advisory

Sash Mukherjee
VP Content & Principal Analyst,
Industry Research

Tim Sheedy
Principal Advisor,
Cloud & AI