ecosystm.

15 17 NOV 2023 | SINGAPORE FINTECH FESTIVAL™

Cyber-Resilience in Finance: People, Policy & Technology

OCTOBER 2023

Ecosystm research reveals a stark reality: 75% of technology leaders in Financial Services anticipate data breaches.

Given the sector's regulatory environment, data breaches carry substantial financial implications, emphasising the critical importance of giving precedence to cybersecurity. This is compelling a fresh cyber strategy focused on early threat detection and reduction of attack impact.

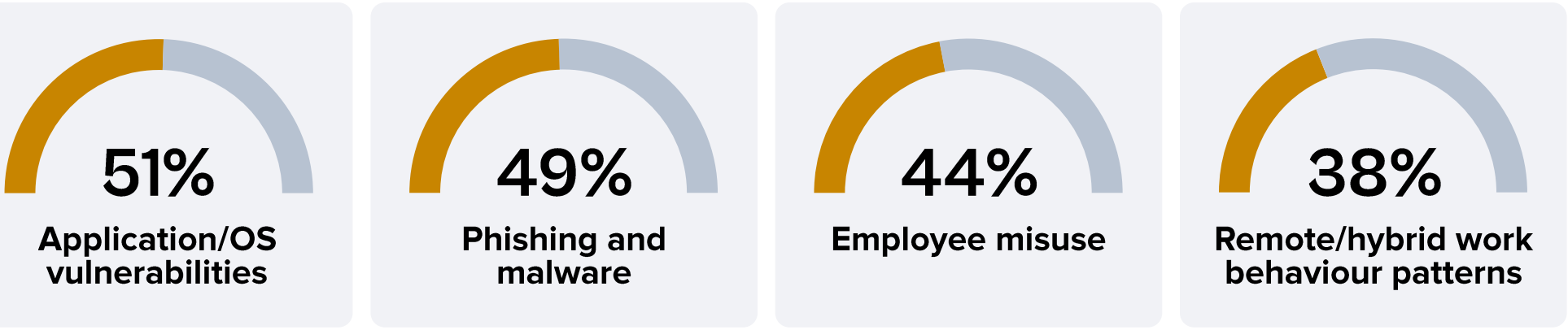
Tech leaders need to build a culture of cyber-resilience, re-evaluate their cyber policies, and adopt technologies that keep them one step ahead of their adversaries – AI lies at the core of the evolved cyber practices.

Biggest CISO Challenges in Finance

The concerns of the BFSI CISO fall into two distinct categories:

- Increase in technology adoption, leading to a proliferation of applications and devices, as well as data access beyond the network perimeter.
- Vulnerabilities originating from employee behaviour, including responses to phishing and malware attacks, as well as both deliberate and inadvertent misuse.

Top Cyber Concerns of BFSI CISOs



Source: Ecosystm Digital Enterprise Study, 2023

Building a Culture of Cyber-Resilience

Financial Services organisations have initiated training and awareness sessions to educate employees about common threats like phishing and data protection best practices.

However, often these programs devolve into mere compliance exercises, raising doubts about their actual impact.

Measures to build a culture of cyber-resiliency:

- Simulated phishing tests and security quizzes are vital to assess employee awareness and identify areas requiring targeted training.
- Establishing company-wide security KPIs that flow from the CEO to every employee are key to emphasise accountability and transparency.
- Creating an environment where employees feel safe reporting security concerns is important for early threat detection and mitigation.

Keeping Cyber Policies Relevant

To ensure employees have a clear understanding of their roles within the broader security framework, it's imperative to establish well-defined security policies and rigorously enforce them.

What a cyber policy should consider:

01 Clear responsibilities for all employees on cyber measures such as the proper use of strong passwords, secure data handling, and the prompt reporting of incidents

02 The principle of least privilege, to help mitigate potential harm stemming from insider threats and inadvertent data exposure

03 Ongoing policy evolution through regular security audits, including technical assessments and evaluations of employee adherence

04 A well-defined incident response plan that is regularly tested and updated, to ensure that every employee is well-versed in their roles and responsibilities during a security incident

Adopting the Right Cyber Technologies

Ecosystm research finds that nearly 70% of Financial organisations intend to adopt AI and automation for security operations, over the next two years.

The volume of incoming threats has grown beyond the capability of human operators to manage manually. This will require a level of automation in the SOC to minimise the routine burden on the security operations team and allow them to focus on high-risk threats.

The Role of AI in Improving Cyber Efficiency

Reducing Alert Fatigue

Cyber tools proliferation means security teams grapple with issues like a lack of centralised control, a high volume of security events, and false positives. Efficient management requires increased automation, addressing alert fatigue and improving risk focus. AI-powered solutions can deprioritise alerts, allowing teams to concentrate on genuine risks.

Taking Corrective Action

AIOps tools not only prioritise alerts but also take action, guiding problems to the right individuals and suggesting operator actions within collaboration tools. They can automatically execute rule-based workflows and learn from past incidents to foresee critical events and their appropriate responses.

The Role of AI in Proactive Cyber Management

1

Threat Intelligence

A comprehensive threat data repository with data from customers and the industry, with insights from dark web research can enhance situational awareness and assist security teams in preparing for future attacks. Regular threat landscape reports keep CISOs well-informed.

2

Network Visibility

This allows monitoring traffic within complex environments, not just at the firewall. ML-driven network traffic anomaly detection detects unusual activities like privilege escalation and container escape. Using AI and adopting a zero-trust approach allows automated device profiling and access control, offering network operators insight into unknown devices and facilitating policy enforcement in segmented networks.

3

Attack Simulation

Automated attack simulations using real-time and real-life scenarios are impactful in alerting organisations of emerging threats. Response planning should include these organisation-wide exercises, that include security, IT operations, and communications teams.

15 17 NOV 2023 | SINGAPORE FINTECH FESTIVAL™

The World's Most Impactful FinTech Event

Policy Finance Technology

GET YOUR FESTIVAL PASS

Ecosystm members are entitled to
20% OFF DELEGATE PASSES

bit.ly/sff23-ecosystm

PROUD KNOWLEDGE PARTNER OF SFF 2023

ecosystm.

Organised by

MAS Monetary Authority of Singapore

ELEVANDI

constellar

In collaboration with

abs