ecosystm

JANUARY 2022

ECOSYSTM BYTES

Shaping your Cyber Practice in 2022

Andrew Milroy

Massively Expanding Attack Surfaces Accelerate Cybersecurity Transformation

Against a backdrop of extended disruption, cybersecurity risks are expanding rapidly and current defences are inadequate. Ransomware attacks are increasing in frequency and impact, focusing more on targets where outages are not an option, such as critical infrastructure and hospitals. Supply chain attacks are creating chaos and has led to a much-needed focus on supply chain vulnerabilities.

As digitalisation continues at a faster pace, cybersecurity is too often, a secondary concern.

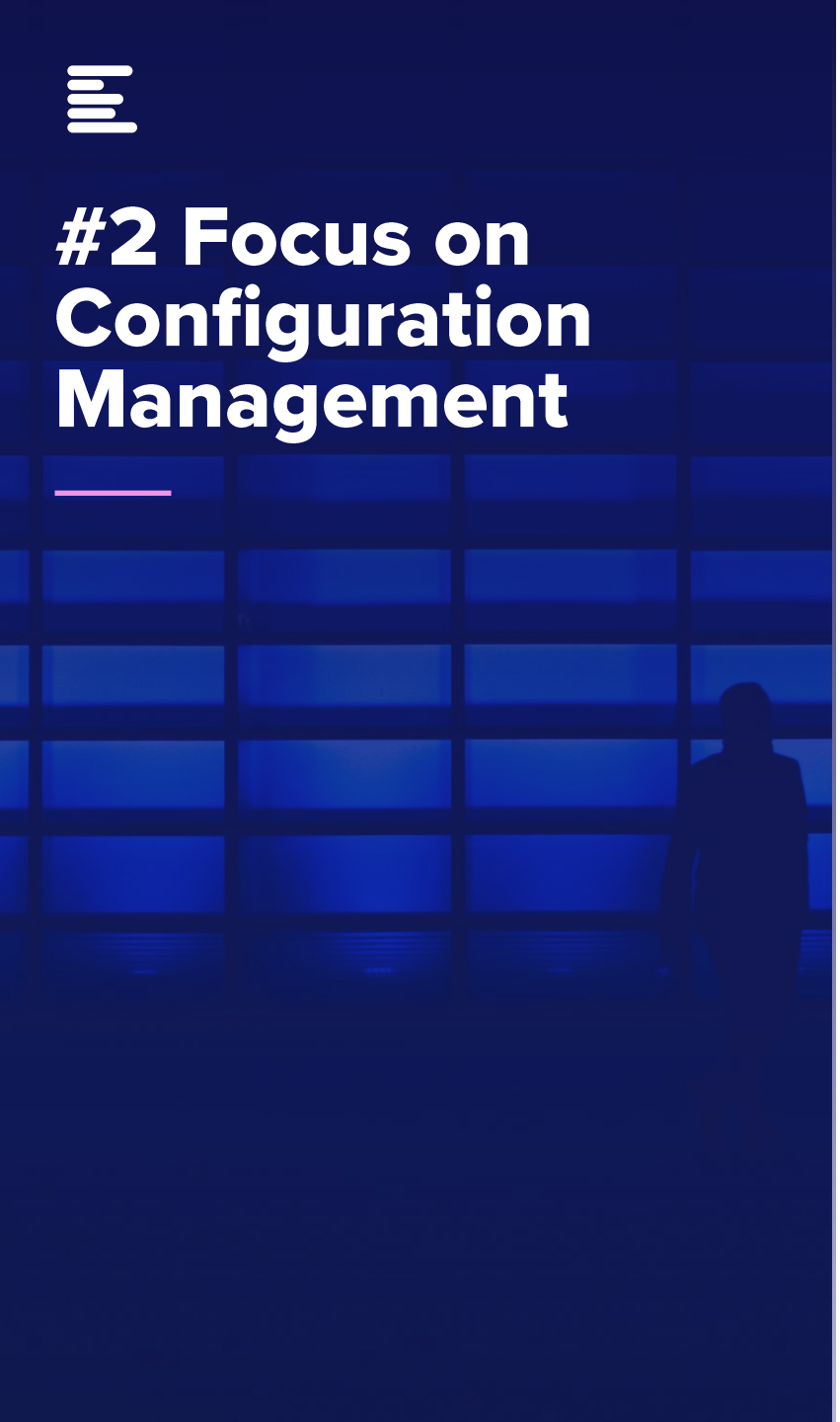
With the acceleration of cloud adoption; widespread remote working; the resulting proliferation of endpoints; and the expansion of attack surface for malicious actors, this is the time for organisations to transform their cybersecurity approaches.

#1 Have CISOs Report Directly into Top Management – Bypassing CIOs

Too often, the interests of the CIO and the CISO conflict. Every digital transformation project driven by a CIO creates an expanded attack surface. CISOs are then expected to put out these metaphorical fires!

Digital transformation projects are increasingly being hijacked by threat actors. CISOs need to be empowered to ensure that security best practices are followed throughout the organisation. For this to happen, they need the support of the business and to operate outside of the IT department which is typically the creator of cybersecurity vulnerabilities.

Give your CISOs more authority and influence in corporate decision-making and frame cybersecurity conversations in the language of the business and of risk.



#2 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 public facing. Incorrect configuration can result in storage offerings such as AWS S3 being exposed. Access to this data can easily be indiscriminately granted to anyone, which can have a devastating impact.

Preventing misconfigurations is critical to ensuring that cybersecurity posture is effectively managed.

#3 Build Resilience Against Ransomware Attacks

The costs of launching a ransomware attack are falling – while the potential rewards are increasing for threat actors. Ransomware as a service (RaaS) kits can be purchased on the dark web for a few hundred dollars and if used repeatedly are likely to find at least one victim. Some organisations have little choice but to pay a ransom when attacked. For example, the healthcare sectors and critical infrastructure companies are highly likely to pay ransoms quickly because the impact of outages for them can be catastrophic. Expect to see ransomware actors target critical infrastructure companies, hospitals, schools, and smaller companies in 2022.

Focus on minimising the damage that can be caused by ransomware attacks. This involves building greater resilience with immutable backup and taking a zero-trust approach.

#4 Migrate Away from a Legacy Perimeter-Based Approach

The traditional network infrastructure model of centralised corporate data centres secured by on-premises network perimeters, doesn't 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.

Develop 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.

#5 Shift to Policy-As-Code

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

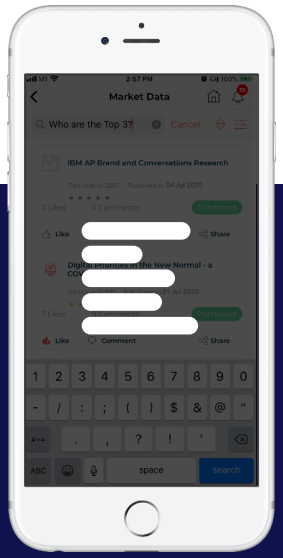
Security by design will become more common as security programs align with DevOps to provide the automation required to secure complex technology environments. Developers will start to see baking security into code, not as an inconvenience, but as a critical part of creating new applications rapidly.

While you may not be able to implement all policies as code, start by targetting access, governance and configuration policies.

Ecosystm Opinion

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

In 2022, attacks on organisations will grow in frequency and intensity. Organisations need to transform their approaches to cybersecurity. This involves embracing new concepts such as zero-trust and Secure Access Service Edge (SASE) as well as a stronger focus on policy as code and human factors.



info@ecosystm360.com

www.ecosystm360.com