CLICK, LISTEN & LEARN

Protecting Critical Infrastructure from Cyberattacks

June 22, 2023

John Hewie
National Security Officer
Microsoft Canada
jhewie@microsoft.com

Microsoft Digital Defence Report 2022:

132 Microsoft contributors

5 Chapters:
The State of Cybercrime
Nation State Threats
Devices and Infrastructure
Cyber Influence Operations
Cyber Resilience

113 Pages of data, analysis, discussion, and actionable insights

https://aka.ms/mddr

Our unique vantage point

37bn
email threats blocked

34.7bn
identity threats blocked

43tn
signals synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

8,500+
engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across 77 countries.

2.5bn
endpoint signals analyzed daily

15,000+
partners in our security ecosystem who increase cyber resilience for our customers.

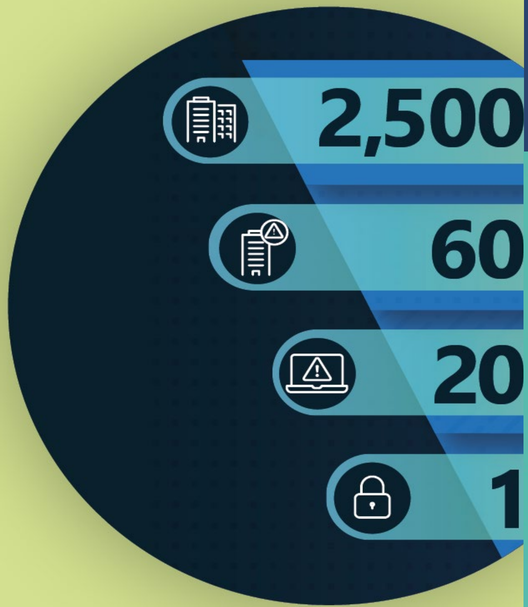
July 1, 2021 through June 30, 2022

The State of Cybercrime: Key takeaways

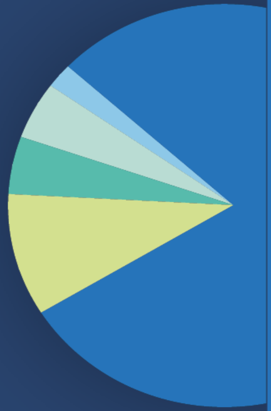
Cybercrime continues to rise as the industrialization of the cybercrime economy lowers the skill barrier to entry by providing greater access to tools and infrastructure.

The threat of ransomware and extortion is becoming more audacious with attacks targeting governments, businesses, and critical infrastructure.

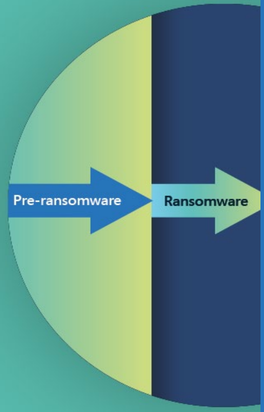
Human operated ransomware is most prevalent, as one-third of targets are successfully compromised by criminals using these attacks and 5% of those are ransomed.



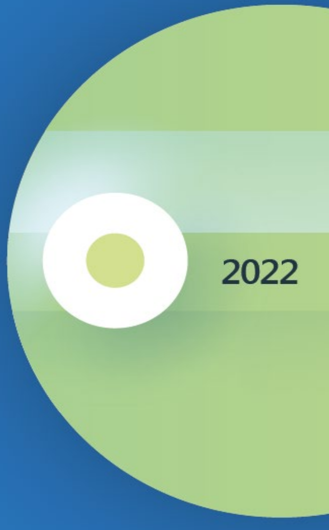
Credential phishing schemes which indiscriminately target all inboxes are on the rise and business email compromise, including invoice fraud, poses a significant cybercrime risk for enterprises.



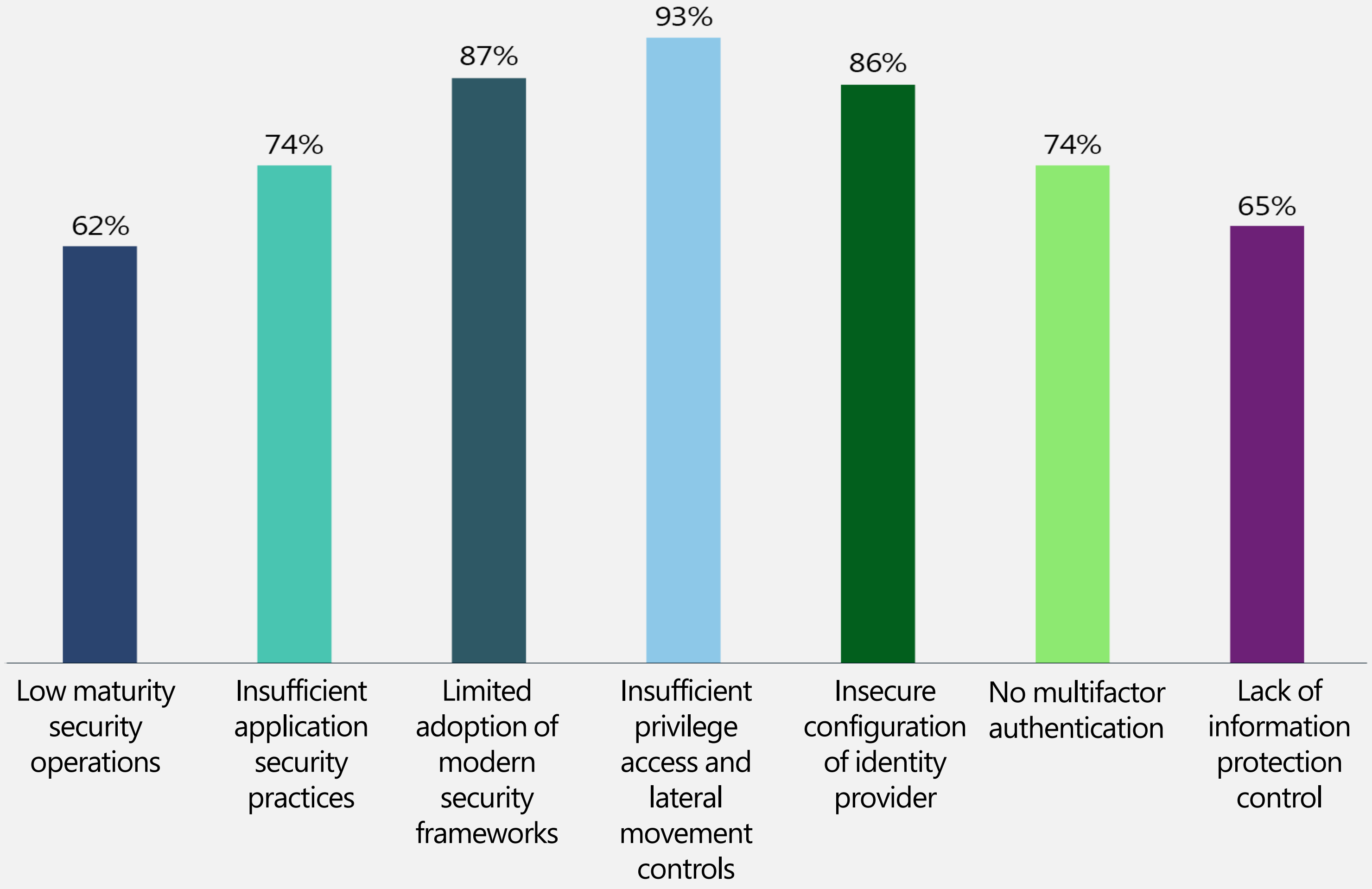
The most effective defense against ransomware includes multifactor authentication, frequent security patches, and Zero Trust principles across network architecture.



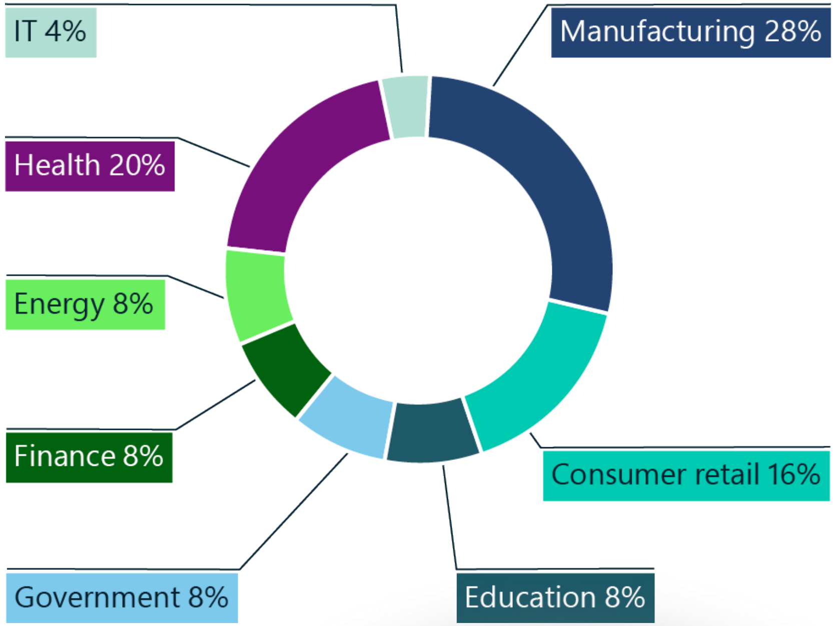
To disrupt the malicious infrastructures of cybercriminals and nation state actors, Microsoft relies on innovative legal approaches and our public
partner



Ransomware insights from frontline responders



Ransomware incident and recovery engagements by industry



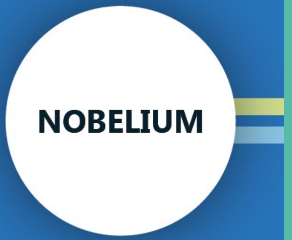
93%

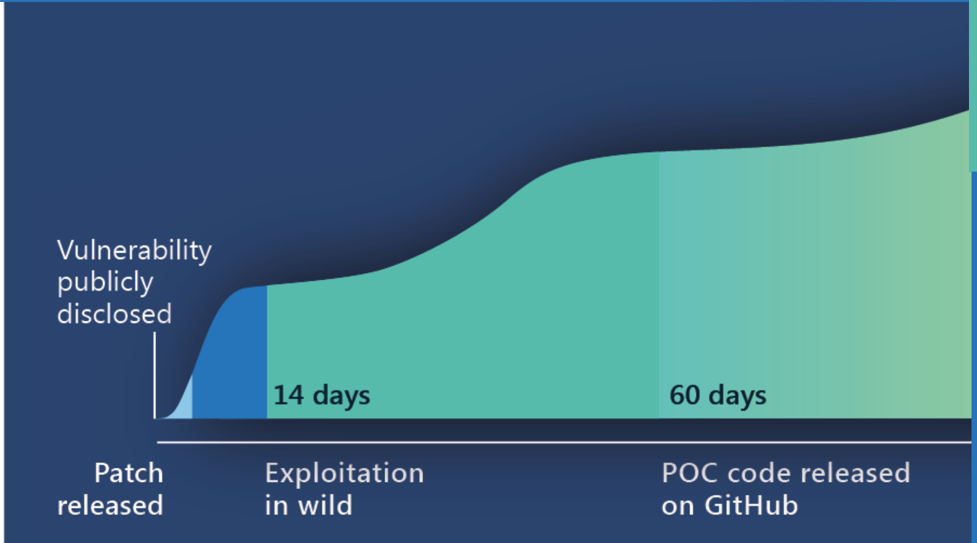
of Microsoft ransomware recovery investigations revealed insufficient controls on privilege access and lateral movement.

Nation State Threats: Key takeaways

Increased targeting of critical infrastructure particularly IT sector, financial services, transportation systems, and communications infrastructure.

IT supply chain being used as a gateway to access targets.





China expanding global targeting especially smaller nations in Southeast Asia, to gain intelligence and competitive advantage.

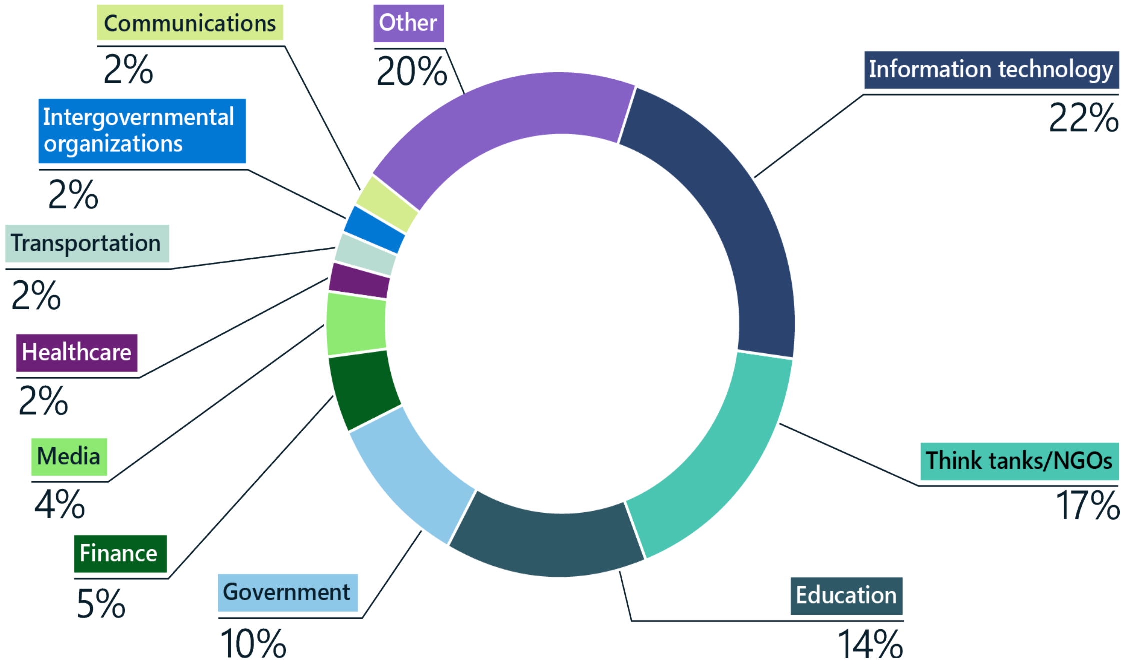
Iran grew increasingly aggressive following power transition, expanded ransomware attacks beyond regional adversaries to US and EU victims, and targeted high profile US critical infrastructure.

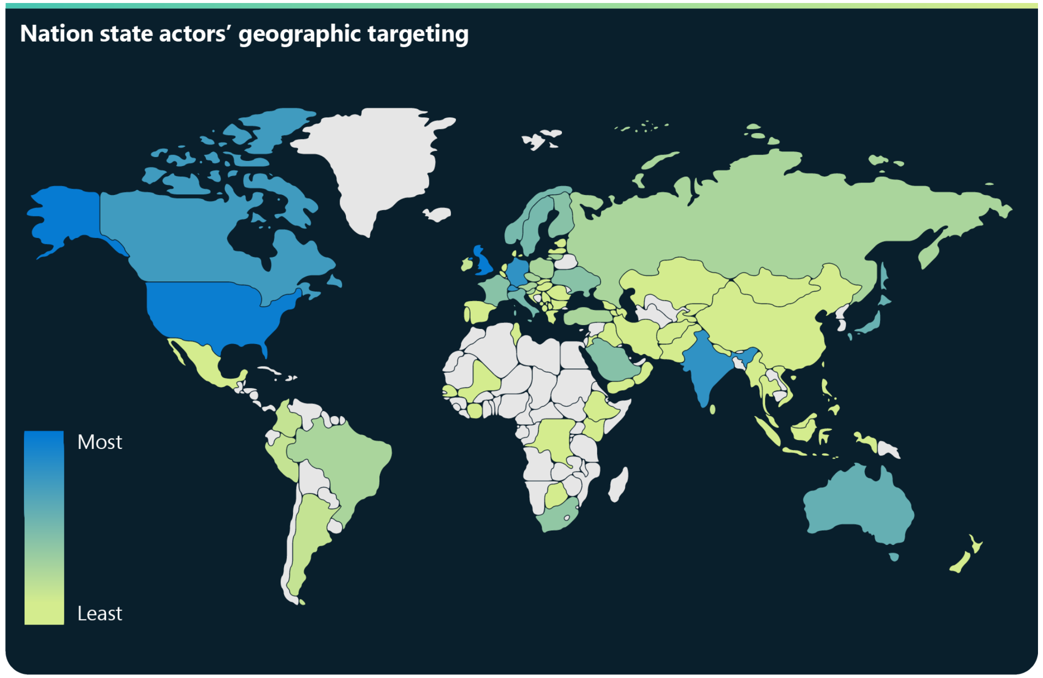
North Korea targeted defense and aerospace companies, cryptocurrency, news outlets, defectors, and aid organizations, to achieve regime's goals: to build defense, bolster the economy, and ensure domestic stability.

Cyber mercenaries threaten the stability of cyberspace as this growing industry of private companies is developing and selling advanced tools, techniques, and services to enable their clients (often governments) to break into networks and devices.

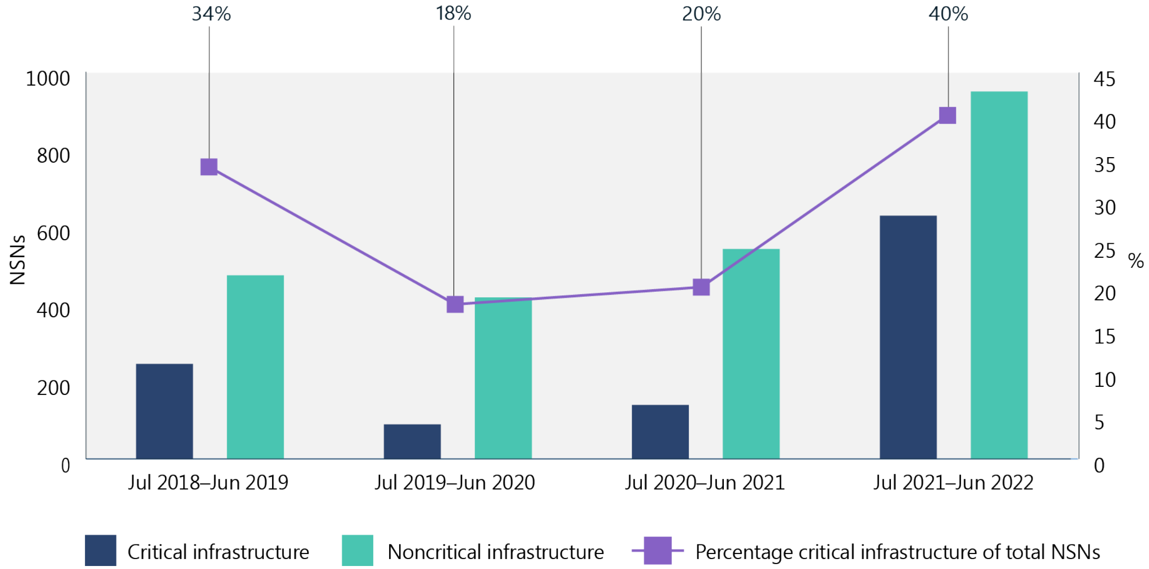
The evolving threat landscape

Industry sectors targeted by nation state actors

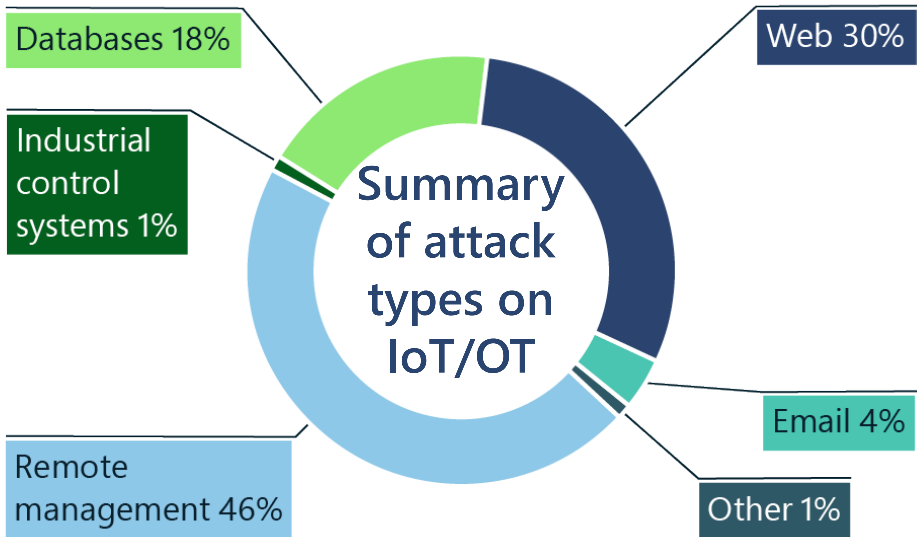



Nation state actors’ geographic targeting

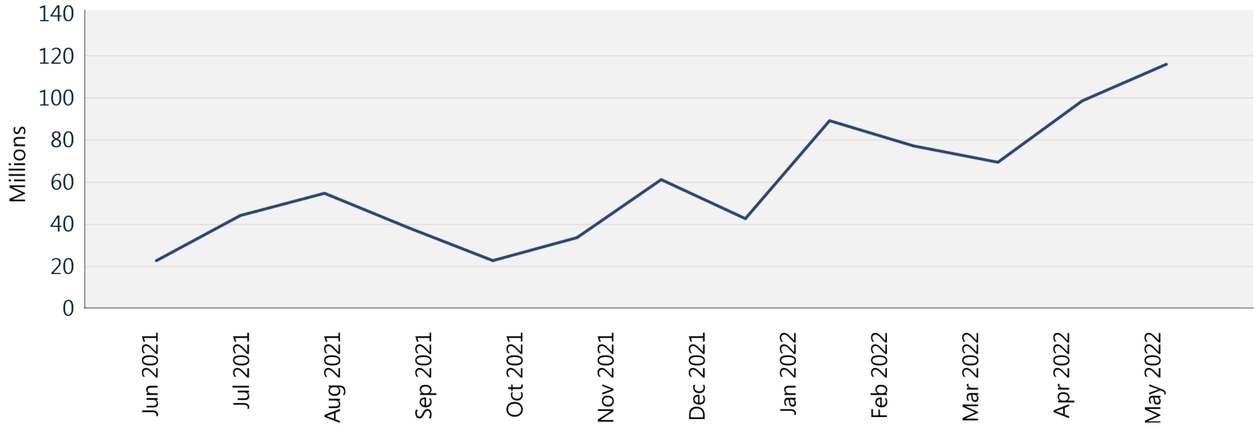
Nation state targeting of critical infrastructure increased in the past year



IoT attacks and weaknesses



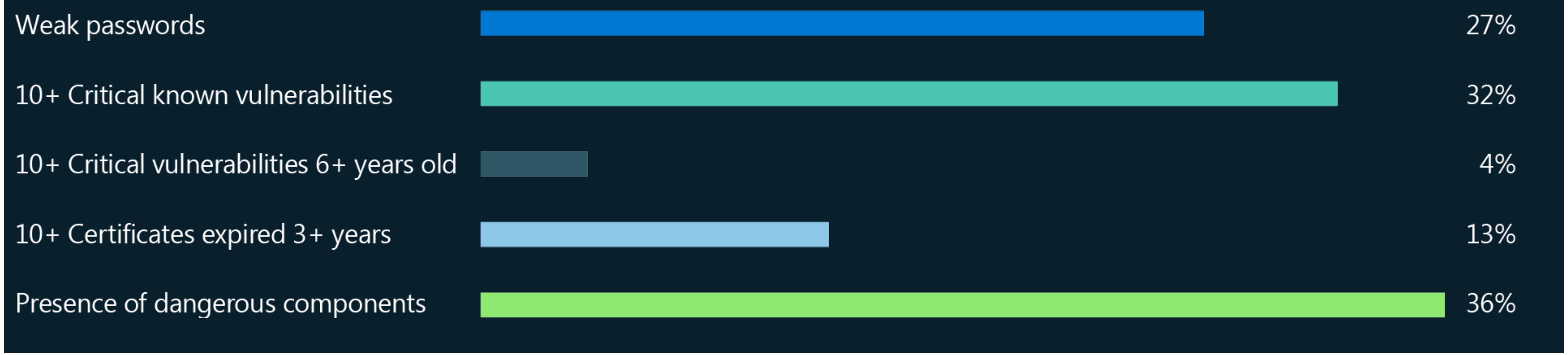
Attacks against remote management devices



32%

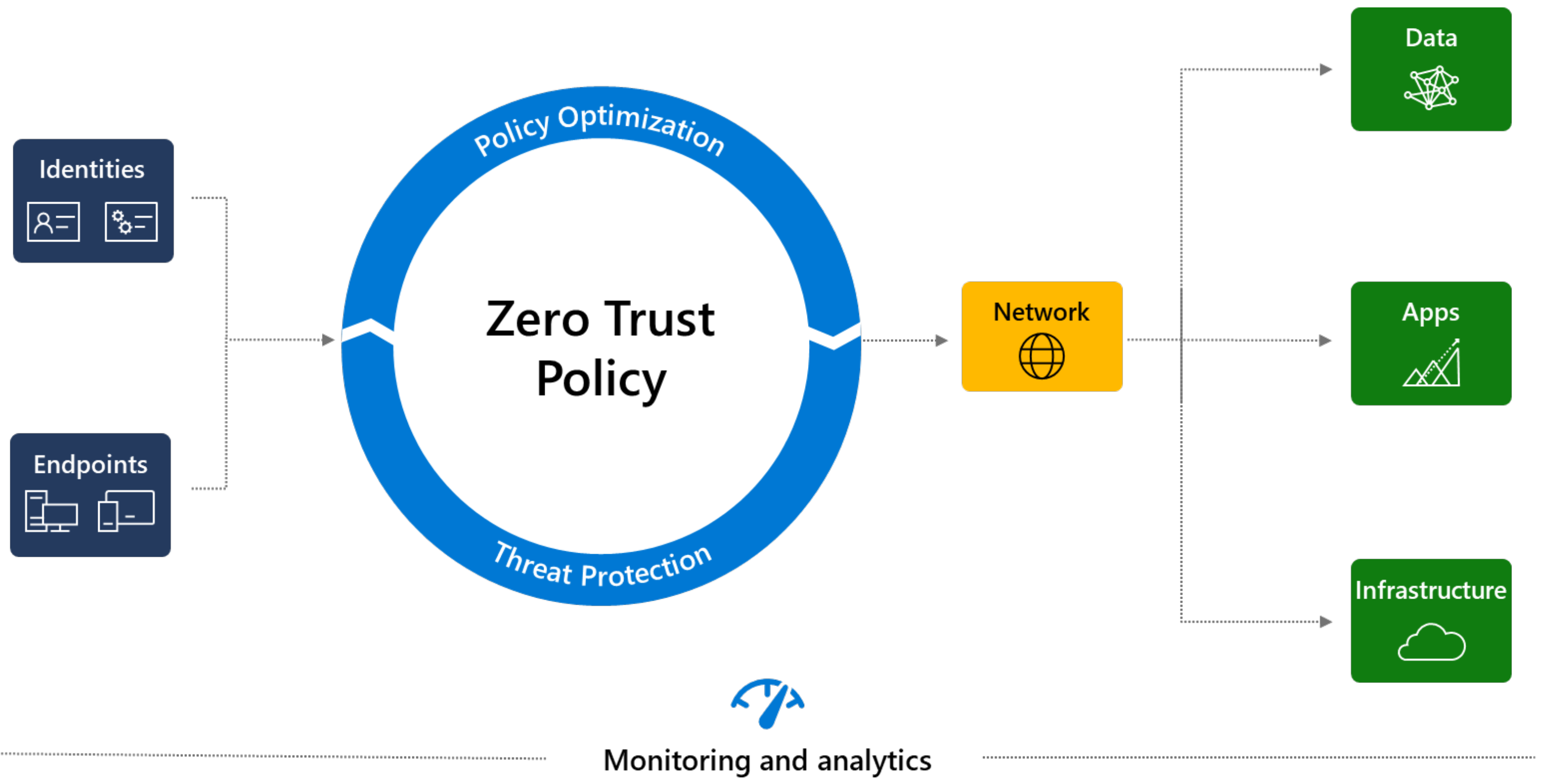
of firmware images analyzed contained at least 10 known critical vulnerabilities.

Security weaknesses in firmware images analyzed:



Secure your organization with a Zero Trust strategy

Increase security assurances for your critical business assets



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Zero Trust Maturity Model

CANADIAN CENTRE FOR CYBER SECURITY

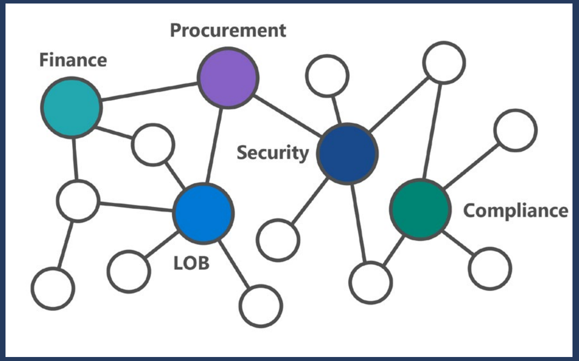
Zero Trust security model - ITSAP.10.008

From: Canadian Centre for Cyber Security

Microsoft

Supplier ecosystem risk management

Siloed environments pose challenges to risk assessment and management



Priorities for a Zero Trust security model for supplier ecosystem risk

- Institute MFA
- Customize solutions
- Greater visibility into who has access

How we think about supply chain

Nine areas of investment for a secure end-to-end supply chain

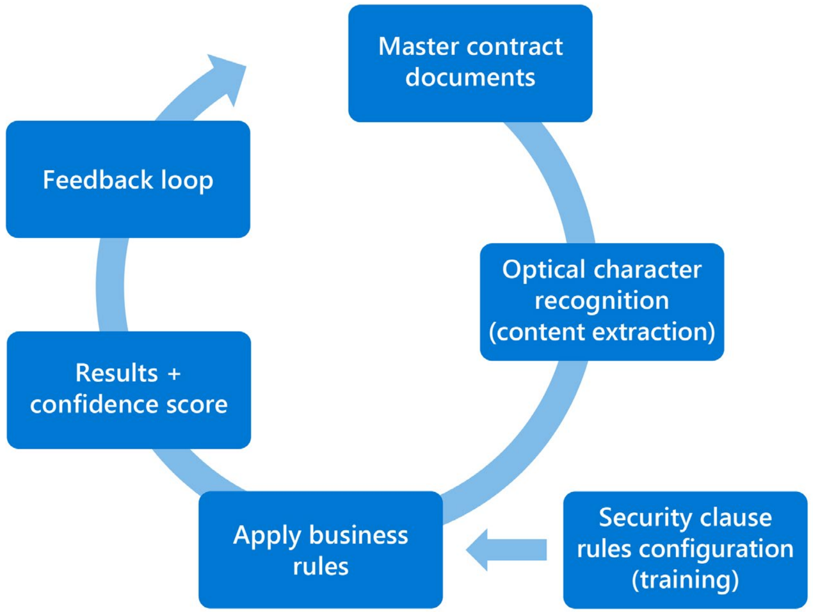
First-party engineering systems for hardware and software	Firmware and driver security	Physical security	Manufacturing security	Logistics security	Supplier security

Trust chain governance and resilience

Security validations and assurances

Monitoring and detections

Leveraging machine learning for continuous security monitoring of suppliers



Master contract documents

Optical character recognition (content extraction)

Apply business rules

Security clause rules configuration (training)

Results + confidence score

Feedback loop

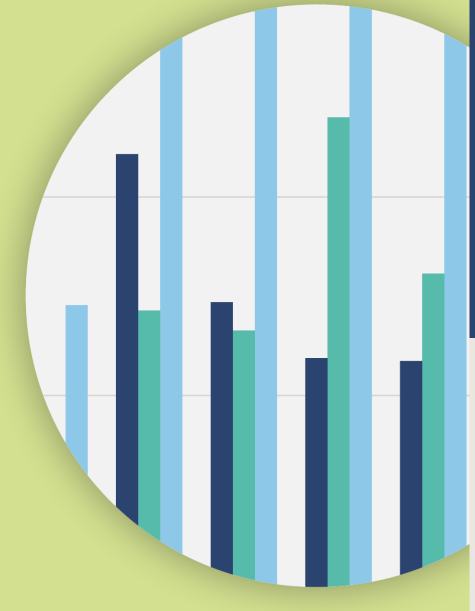
Cyber Resilience: Key takeaways

Effective cyber resiliency requires a holistic, adaptive approach to withstand evolving threats to core services and infrastructure.

Modernized systems and architecture are important for managing threats in a hyperconnected world.

Basic security posture is a determining factor in advanced solution effectiveness.

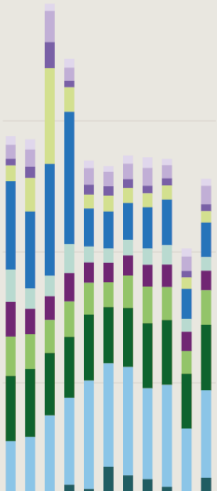
While password-based attacks remain the main source of identity compromise, other types of attacks are emerging.



The human dimension of resilience to cyber influence operations is our ability to collaborate and cooperate.

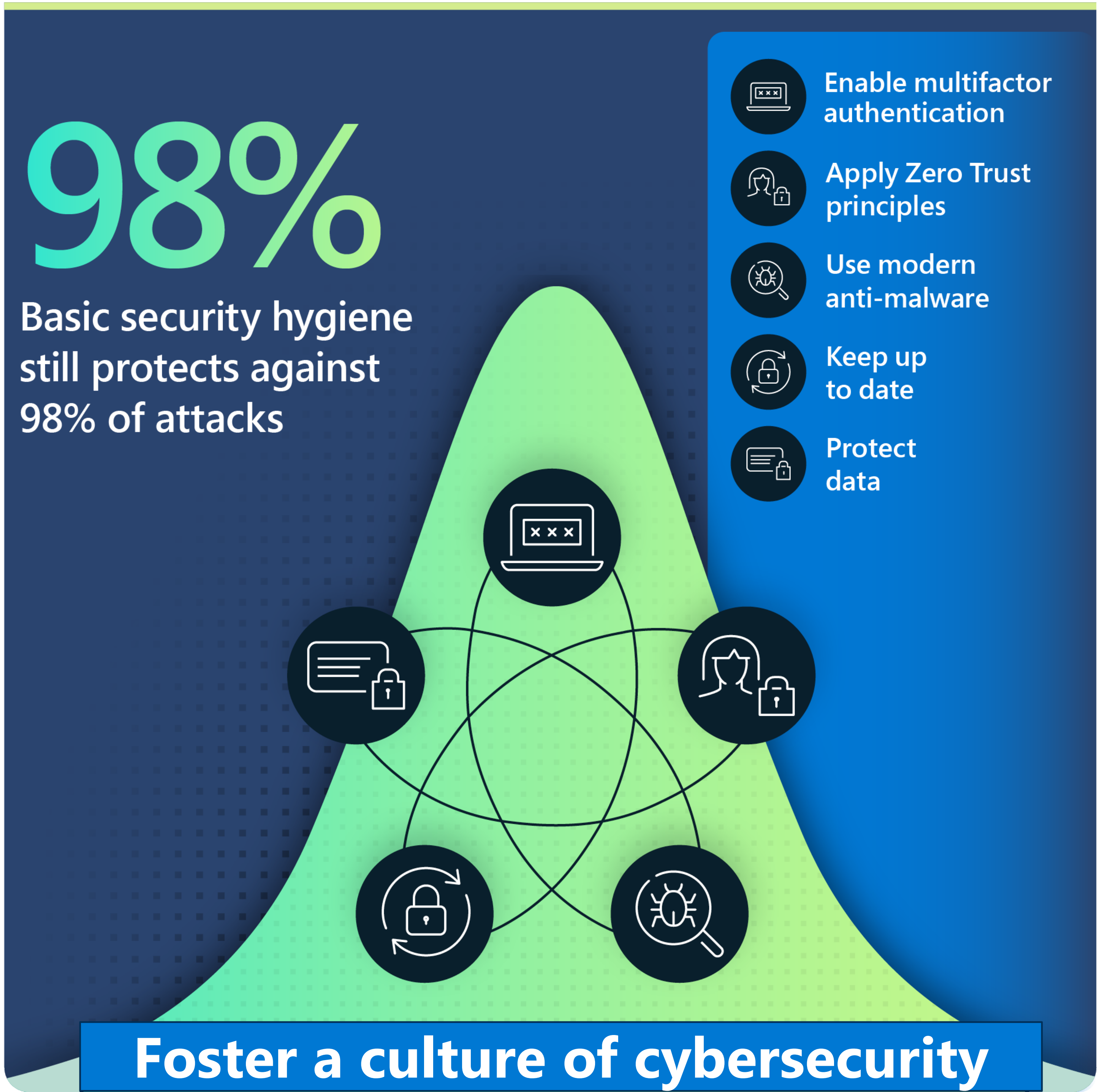
The vast majority of successful cyberattacks could be prevented by using basic security hygiene.

Over the past year, the world experienced DDoS activity that was unprecedented in volume, complexity, and frequency.



The cyber resilience bell curve

Resilience success factors every organization should adopt



98%

Basic security hygiene still protects against 98% of attacks

- Enable multifactor authentication
- Apply Zero Trust principles
- Use modern anti-malware
- Keep up to date
- Protect data

Foster a culture of cybersecurity

Microsoft

Illuminating the threat landscape
and empowering a digital defense.

THANK YOU

- Learn more: https://microsoft.com/mddr
- Dive deeper: https://blogs.microsoft.com/on-the-issues/
- Stay connected: @msftissues and @msftsecurity