



Texas Information Security Forum

ISF 2017, April 11, 2017 – Palmer Events Center, Austin TX

Abstract Title: “A day in the life after you implement the Identify, Detect, Protect, Respond & Recover Framework”

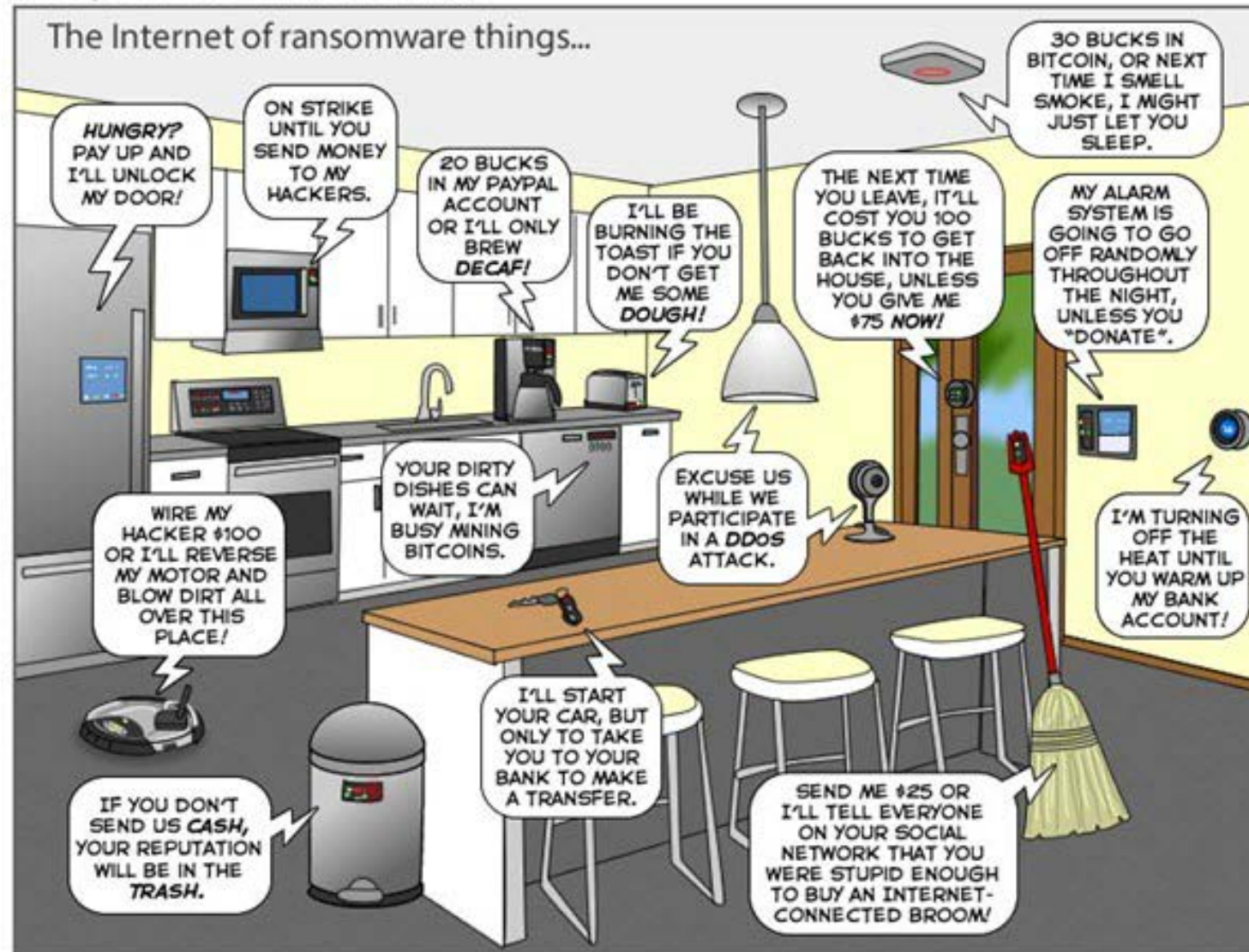
Ned Miller

Chief Technology Strategist | Office of the CTO | US Public Sector
ned_miller@mcafee.com | Direct: 571.355.5887



IoT + Ransomware = Internet of Ransomware things...

The Joy of Tech™ by Nitrozac & Snaggy



Source: <http://www.geekculture.com/joyoftech/joyarchives/2340.html>

Agenda

- Detect, Protect, Respond & Recover... What's Next?
- Cyber Attack Evolution
- Emerging Trends and Threats in Government
- Grobman's Curve – Security Effectiveness Lifecycle
- Security & The Acquisition Lifecycle
- Changing the game for a new era
- Alignment to the NIST RMF Mappings?
- NIST RMF the “After Life”... Interoperability, Orchestration and Automation

Detect, Protect, Respond... What's Next?

NIST Framework Core

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure

NIST Framework Recommendations for Establishing or Improving a Cyber Security Program... 7-Step Program!

1. Prioritize & Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze and Prioritize Gaps
7. Implement an Action Plan

Security's Perfect Storm...

Exponential Attack Surface Growth

By 2020 there will be 26 smart objects for every living person and 5000x more stored bytes than grains of sand on Earth

Intel forecast / IDC

Business Realities

Linear Budgets
Skillset Shortages
Compliance & regulatory
Competitive Pressures

Fragmented Security Market

1400 Security solution vendor offerings to assess and secure an environment

Intel Security

Time Imperative

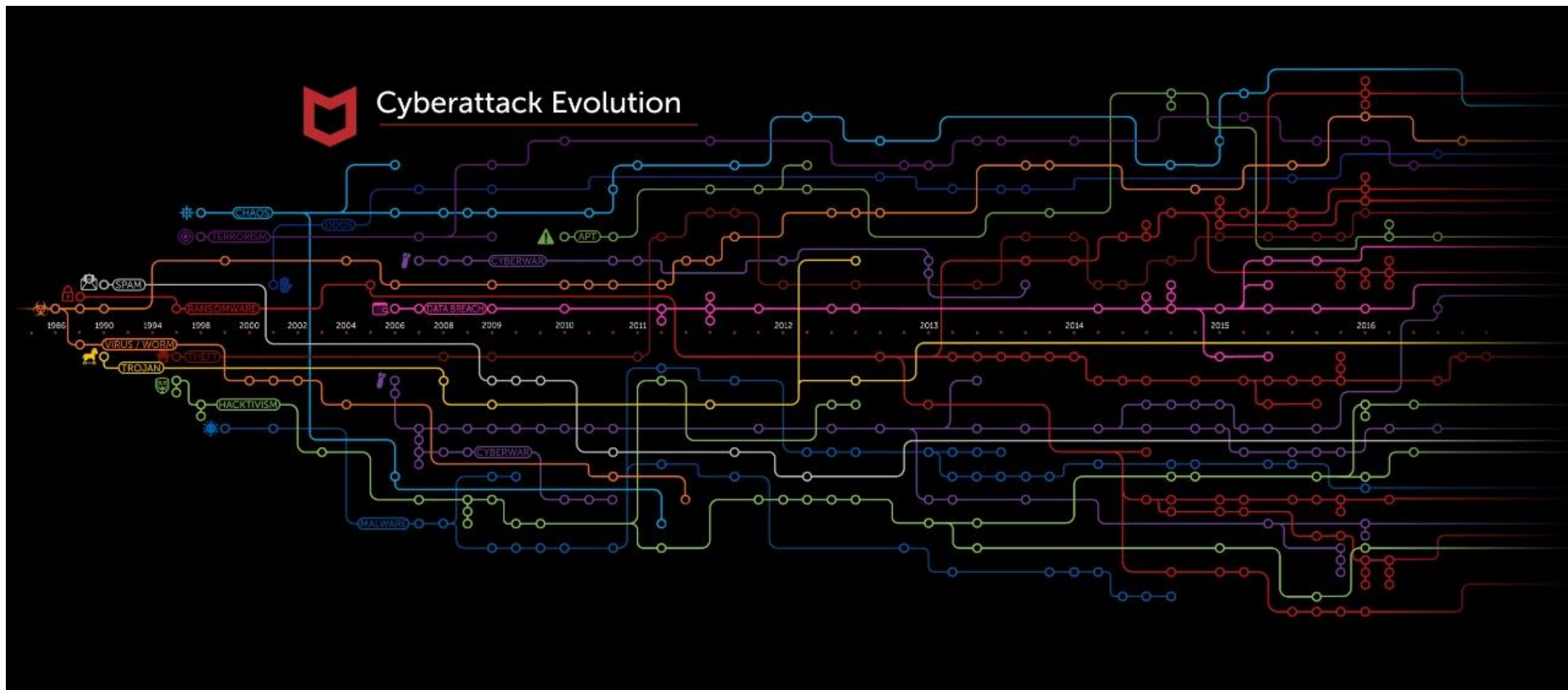
- Organizations compromised in minutes
 - Dwell times lasting for months
 - Damage can be catastrophic

Industrialization of Cybercrime

Breaches up 55% year over year
30% of attacks are targeted

Verizon DBIR 2015 / Intel Security Golden Hour Survey 2016

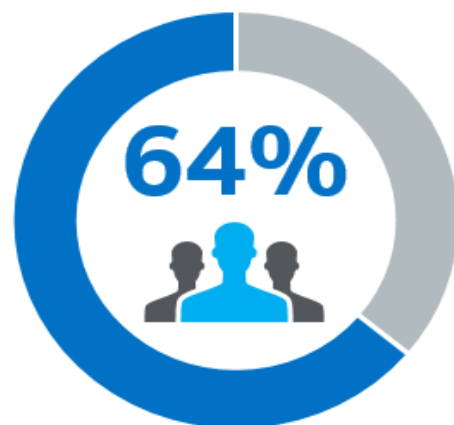
Evolution Fast, Response? Mixed.



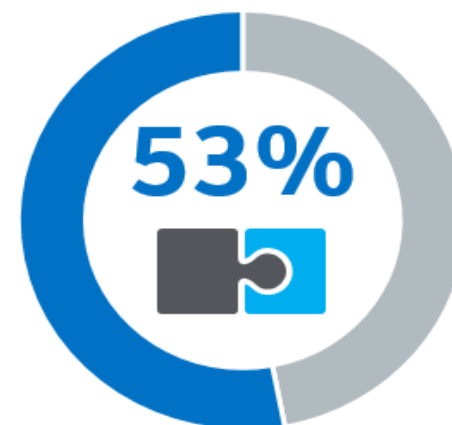
Implications of Technology Sprawl



62% believe security posture is reduced overall



64% cite excessive in-house training burden



53% develop their own integration technologies

Frost & Sullivan, The 2015 (ISC)² Global Information Security Workforce Study

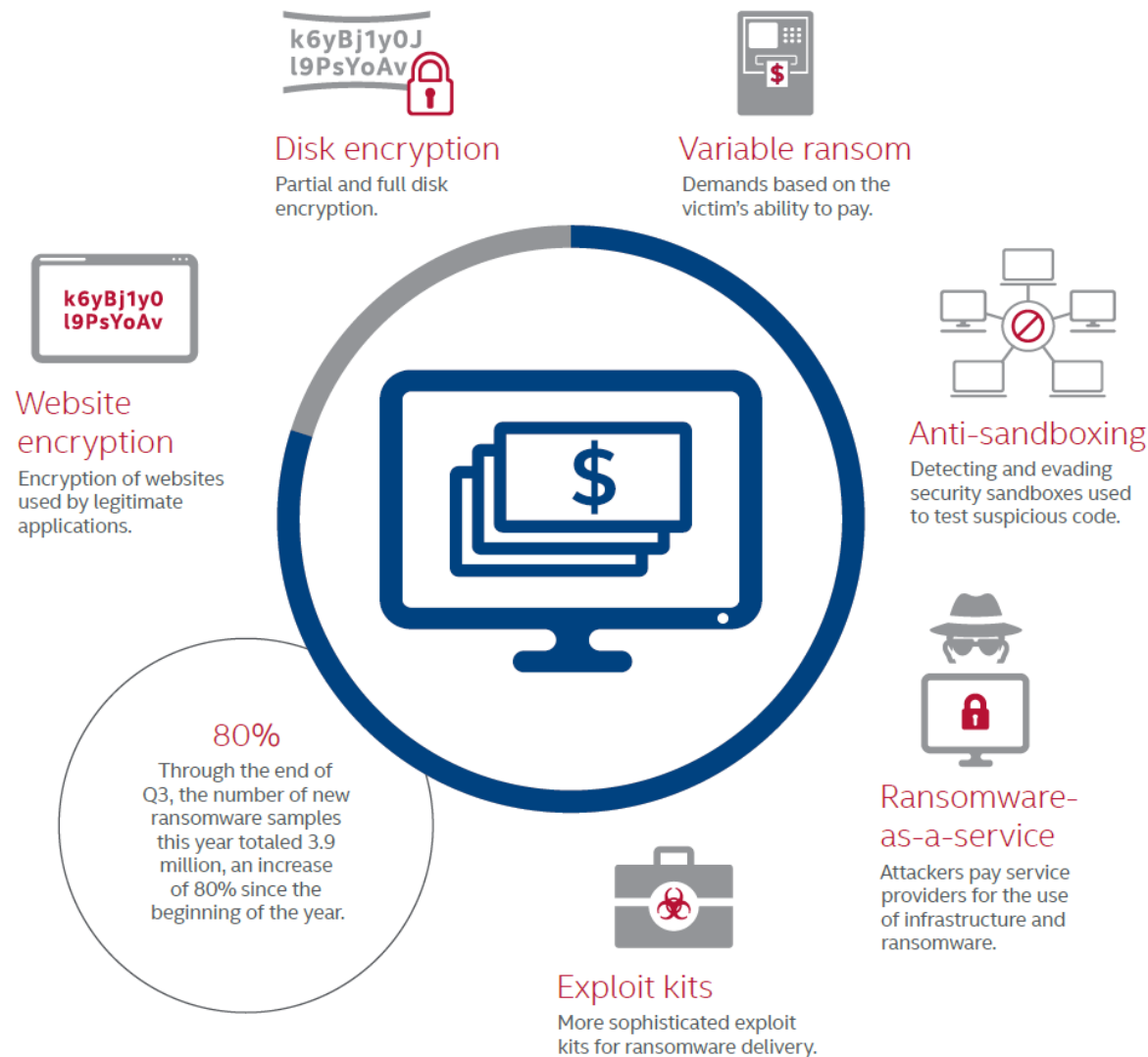
Emerging Trends and Threats in Government...

Trends

- Machine Learning becomes Mainstream¹
- Ransomware-As-a-Service(RaaS)²
- Increased alignment with NIST CSF
 - POTUS' Draft Cyber EO³
 - House Bill for CSF outcome-based metrics⁴
 - FISMA Annual Report to Congress – FY16⁵

Threats

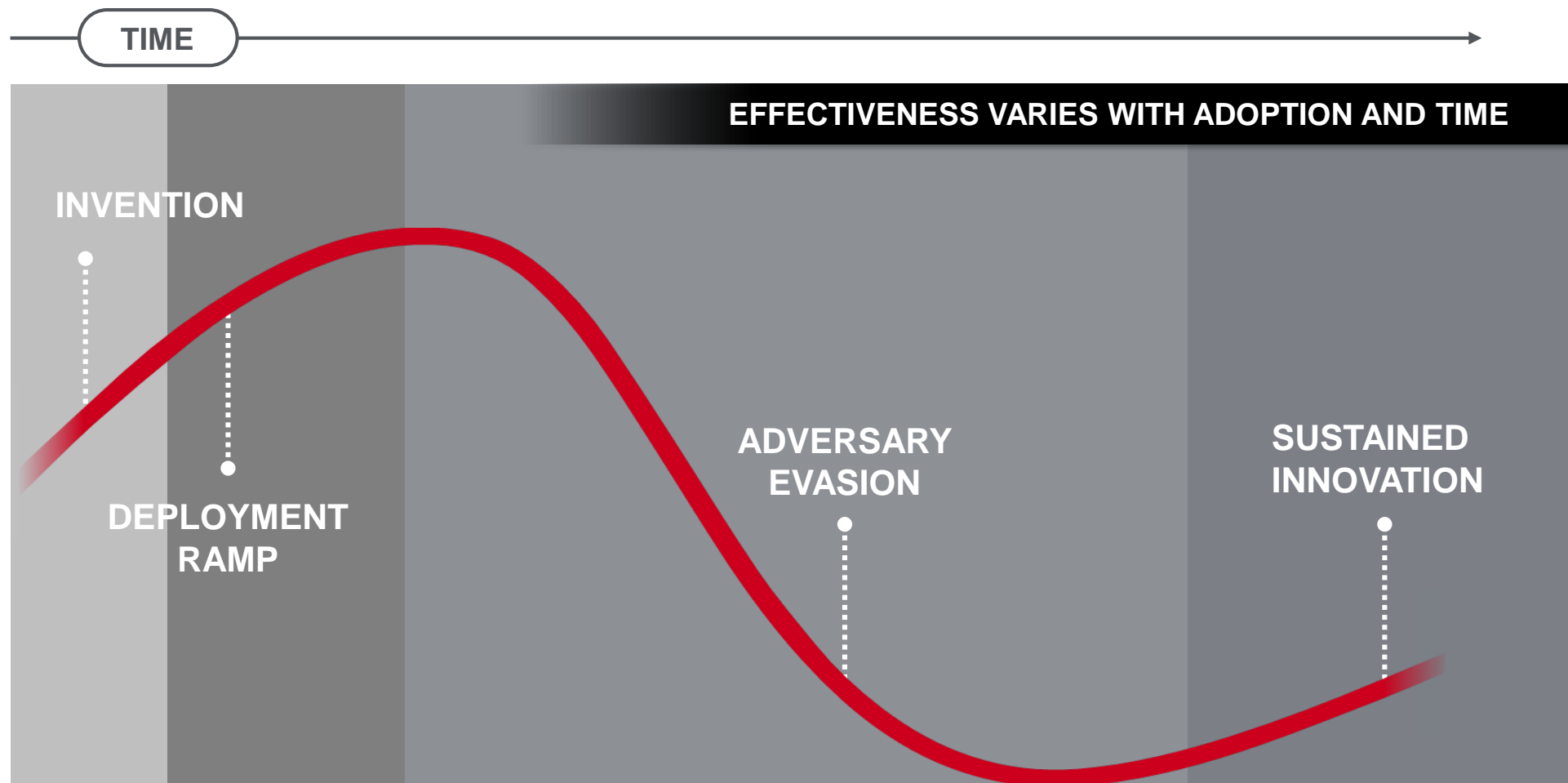
- Increased Ransomware targeting governments entities
 - Ohio Government Shutdown⁶
 - Middle Eastern Government for Political Purposes



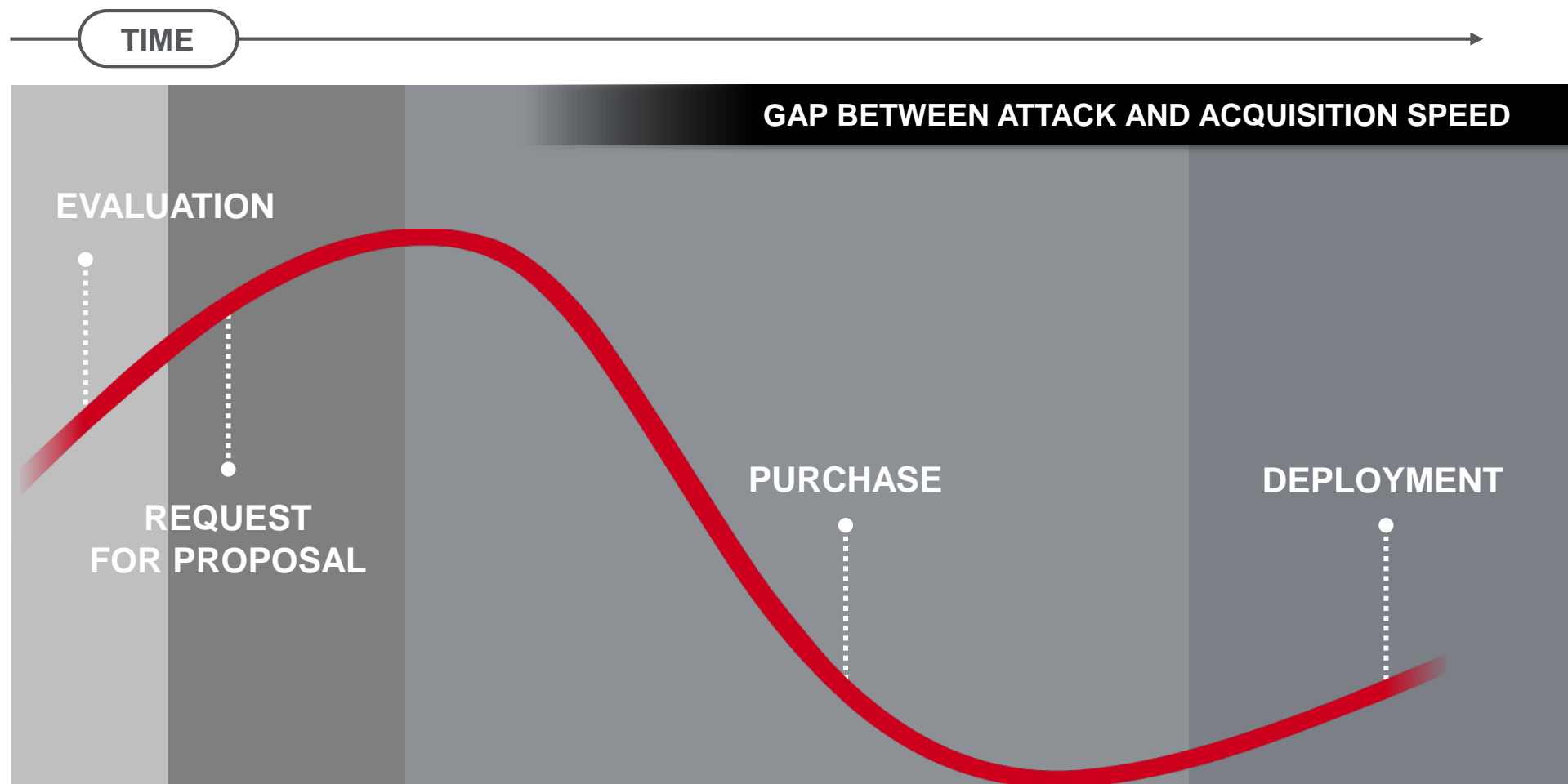
NIST Cyber Security Framework(CSF) : <https://www.nist.gov/cyberframework>

Grobman's Curve

From *The Second Economy*



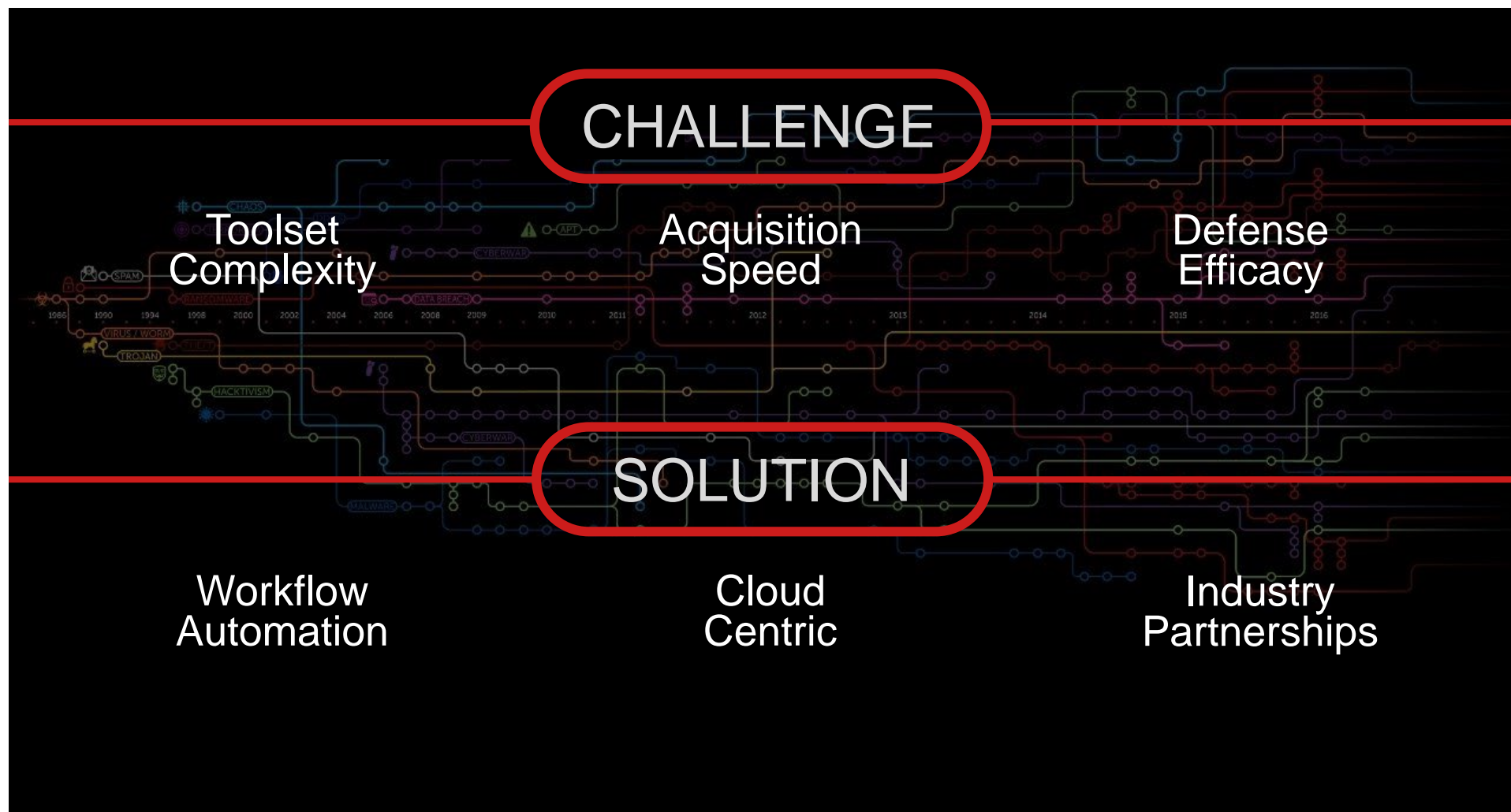
Acquisition Cycle



A More Realistic View



Changing the Game...



NIST Cyber Security Framework Mapping

CSF Function	Category	Cyber Solution Mapping	McAfee Solution	McAfee SIA Partners
Identify (ID)	<ul style="list-style-type: none"> ✓ Asset Management ✓ Business Environment ✓ Governance ✓ Risk Assessment ✓ Risk Management Strategy 	<ul style="list-style-type: none"> - Application Performance Management - Network Performance Management - Network Infrastructure Security Management - Governance, Risk, and Compliance (GRC) Tools - Security Information & Event Management (SIEM) 	<ul style="list-style-type: none"> - <i>Application Control</i> - <i>Enterprise Security Manager(ESM)</i> - <i>McAfee Web Gateway(MWG)</i> - <i>Cloud Access Security Broker(CASB)</i> - <i>Network Security Manager(NSM)</i> - <i>Threat Intelligence Exchange (TIE)</i> 	<ul style="list-style-type: none"> - Aruba Network - Lumeta - Redseal Networks - Tenable - Qualys - Vmware Airwatch - White Cyber Knight
Protect (PR)	<ul style="list-style-type: none"> ✓ Access Control ✓ Awareness and Training ✓ Data Security ✓ Information Protection Processes & Procedures ✓ Maintenance ✓ Protective Technology 	<ul style="list-style-type: none"> - Full Disk Encryption(FDE) - Removable Media and File and Folder Encryption - Next Generation Firewall (NGFW) - Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) - Network Access Control (NAC) - Web & Email Gateways / Forward Proxy - App Delivery Controller (ADC) / Reverse Proxy - Web Application Firewall (WAF) - Data Loss Prevention (DLP) - Security Information & Event Management (SIEM) - Privileged User Access Control - Role Based Data Encryption - Unstructured Data Protection 	<ul style="list-style-type: none"> - <i>McAfee Complete Data Protection</i> - <i>Host Intrusion Prevention for Desktop/Server</i> - <i>Enterprise Security Manager</i> - <i>Network Security Platform(NSP)</i> - <i>McAfee Web Gateway(MWG)</i> - <i>McAfee Active Response</i> - <i>Security for Microsoft SharePoint</i> - <i>Security for Email Servers</i> 	<ul style="list-style-type: none"> - Avecto - Beyond Trust - Boldonjames - Bowbridge - CheckPoint - CyberArk - ForcePoint - HyTrust - Lieberman - Logbinder - Lumeta - MobileIron - Phishme - Titus - Vormetric
Detect (DE)	<ul style="list-style-type: none"> ✓ Anomalies and Events ✓ Security Continuous Monitoring ✓ Detection Processes 	<ul style="list-style-type: none"> - NGFW - IPS / IDS - NAC - Web & Email Gateways / Forward Proxy - ADC / Reverse Proxy / WAF - DLP - Endpoint Threat Detection - Network Behavior Analysis - Honeypots - Sandbox Analysis - SIEM 	<ul style="list-style-type: none"> - <i>Network Security Platform(NSP)</i> - <i>Cloud Threat Detection(CTD)</i> - <i>DLP Discover</i> - <i>DLP Network</i> - <i>DLP Prevent</i> - <i>Endpoint Network Security(ENS)</i> - <i>Dynamic Application Containment</i> - <i>RealProtect</i> - <i>Network Threat Behavior Analysis (NTBA)</i> - <i>Advanced Threat Defense(ATD)</i> - <i>Cloud Threat Detection(CTD)</i> - <i>Enterprise Security Manager (ESM)</i> - <i>Advanced Correlation Engine</i> 	<ul style="list-style-type: none"> - Aruba Networks - Attivo Networks - Cloudera - Core Security - Exabeam - Interset - TrapX
Respond (RS)	<ul style="list-style-type: none"> ✓ Response Planning ✓ Communications ✓ Analysis ✓ Mitigation ✓ Improvements 	<ul style="list-style-type: none"> - Endpoint Threat Detection and Response (ETDR) - Network Behavior Analysis - GRC Tools - Local/Global Threat Feed Tools - Security Operations Center (SOC) Automation 	<ul style="list-style-type: none"> - <i>Endpoint Network Security(ENS)</i> - <i>Network Threat Behavior Analysis (NTBA)</i> - <i>Threat Intelligence Exchange (TIE)</i> - <i>Global Threat Intelligence (GTI)</i> - <i>ePO Orchestrator</i> 	<ul style="list-style-type: none"> - Ayehu - Cyber Phantom - Demisto - Guidance EnCase - ThreatConnect
Recover (RC)	<ul style="list-style-type: none"> ✓ Recovery Planning ✓ Improvements ✓ Communications 	<ul style="list-style-type: none"> - Data replication and backup - DR COOP Sites 		

NIST Risk Management Framework – The After Life...

The only way this can possibly work is through interoperability, orchestration & automation!

- NIST Baldrige Cyber Security Excellence Builder
- NIST 800 Series - Continuous Monitoring is a fan favorite!
- Cloud Security – Lets not forget FedRAMP!
- SANS/CIS TOP 20
- Cyber Kill Chain Exercise
- Value Management – Make your vendors work with you on this effort!
- Establish a Formal Cyber Scorecard – Persona Based, Frequency Daily/Weekly/Monthly
- Establish a third party relationship for annual penetration testing
- Run cyber war ranges, exercise your established policies and see where SOP breaks
- Rinse and Repeat as often as the organization can stand it!

Further References

Worth Reading

1. Google Cloud Platform – Machine Learning Services
 - <https://cloud.google.com/products/machine-learning/>
2. Ransomware as a Service fuels explosive growth
 - <http://www.csoonline.com/article/3146537/security/ransomware-as-a-service-fuels-explosive-growth.html>
3. Draft Executive Order - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
 - https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/feb2017/cs02082017_Draft_Cyber_EO.pdf
4. Bill Seeks Metrics for NIST Cybersecurity Framework
 - <http://www.bankinfosecurity.com/bill-seeks-metrics-for-cybersecurity-framework-a-9744>
5. FISMA Report To Congress March 10, 2017
 - https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf
6. Ransomware completely shuts down Ohio town government
 - <https://techcrunch.com/2017/02/02/ransomware-completely-shuts-down-ohio-town-government/>
7. Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1
 - <http://www.governor.ny.gov/news/governor-cuomo-announces-first-nation-cybersecurity-regulation-protecting-consumers-and>

Thank you!



e-mail: ned_miller@mcafee.com

Learn more at:

<http://www.mcafee.com>

<https://securingtomorrow.mcafee.com>