MOSSADAMS

The Importance of IT Controls & Preparing for Cyberattacks

April 4, 2019

Presenters

Colin Wallace

Partner | Moss Adams LLP

colin.wallace@mossadams.com

Francis Tam

Partner | Moss Adams LLP

francis.tam@mossadams.com

Presenter Bios

Colin Wallace, Partner

CPA, CISA, CIA, CFE, CFF, CGAP

Colin has provided management consulting and internal audit services to public, private, government, and not-for-profit organizations since 2002. He has organized and performed financial, operational, and compliance audits throughout the United States and abroad, and has worked on all aspects of the internal audit process including planning, analysis, reporting, and project management. Colin has led numerous fraud investigations involving misappropriation and misuse of company assets, the Foreign Corrupt Practices Act, and management override of internal controls. In addition, he has managed significant SOC and SOX 404 assessment projects from initial implementation to final reporting. Colin is an active member of the firm's Technology, Communications, and Media Group and is a leader of the firm's forensic and investigative services team. He currently serves as the quality control practice leader for the Business Risk Services group.

Presenter Bios

Francis Tam, Partner

CPA, CISM, CISA, CITP, CRISC, PCIP, PCI QSA

Francis is a partner in the IT Auditing and Consulting group with Moss Adams. He has more than 20 years of experience performing information security and technology audits. Francis specializes in risk mitigation activities relating to IT, including internal control reviews, systems integration control, information security services, secure e-banking, information security risk analysis, business continuity planning, and IT project management review and oversight. In addition to his extensive information risk and security audits and consulting experience, Francis has accumulated significant experience in financial, compliance, operational, and information system audits, and frequently serves as the concurring or lead engagement reviewer for the firm's SOC audit engagements.

Agenda

- Why Should Accounting and Finance Personnel Care about IT Controls?
  - Why is IT Important to Financial Statements?
  - What are the IT Risks?
  - Application Controls
  - Key Reports
  - How Should Accounting and Finance Personnel Be Involved in IT?
- The State of Cybersecurity
  - Top Cybersecurity Threats
  - Are You Prepared for a Cyberattack or Breach Attempt?

Objectives

- Understand the importance of IT controls and how they can impact the production of financial statements, both positively and negatively
- Define key controls related to security and access, change management, system development, and operations
- Describe the difference between IT General Controls (ITGCs) and Application Controls
- Understand the importance of key reports
- Understand how Accounting and Finance personnel should be involved in IT controls and know how those IT controls are established
- Define the actions that can be taken to reduce the likelihood and/or magnitude of a cybersecurity event

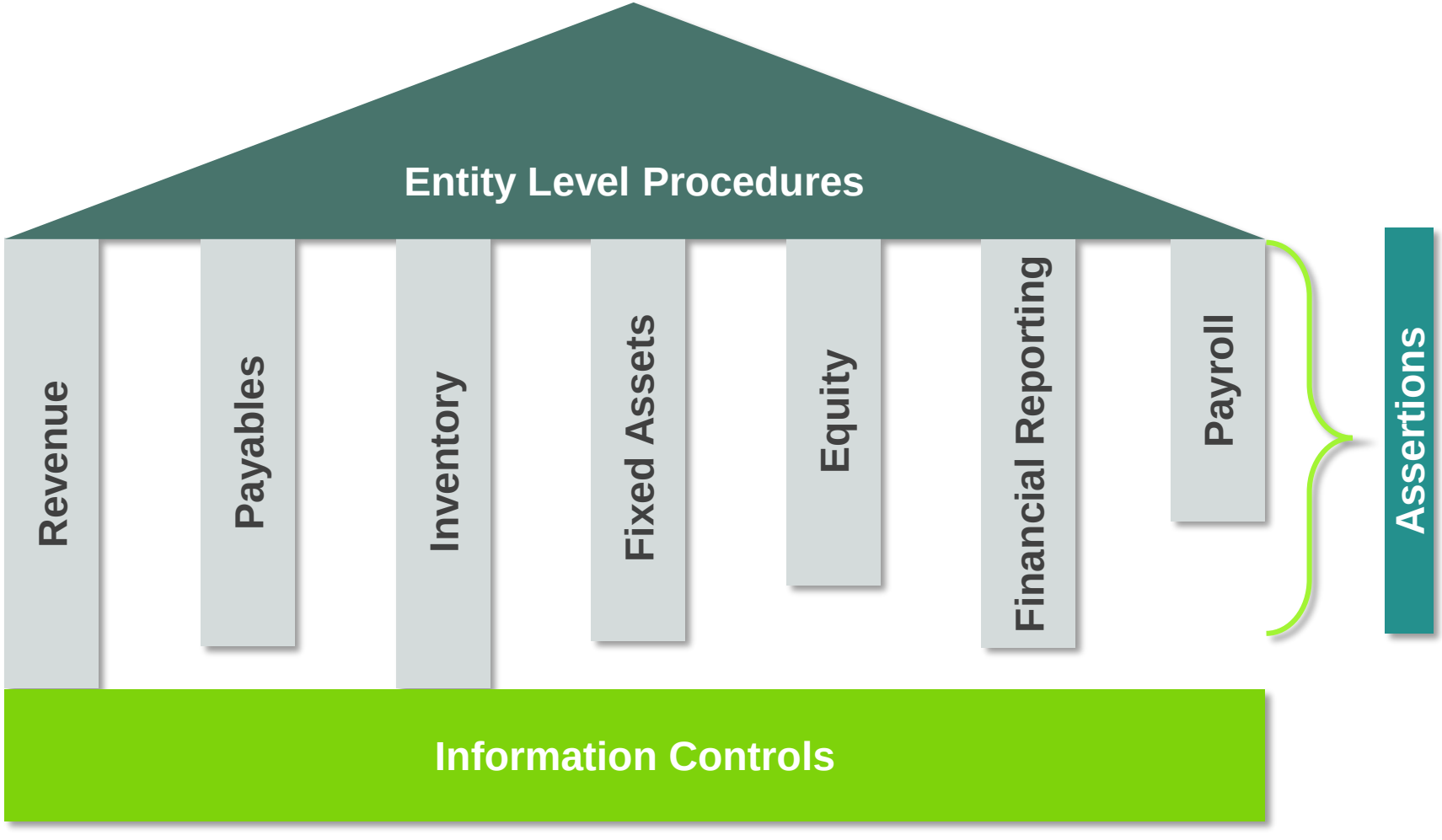
MOSSADAMS

Why Should Accounting and Finance Personnel Care about IT Controls?

Why is IT Important to Financial Statements?

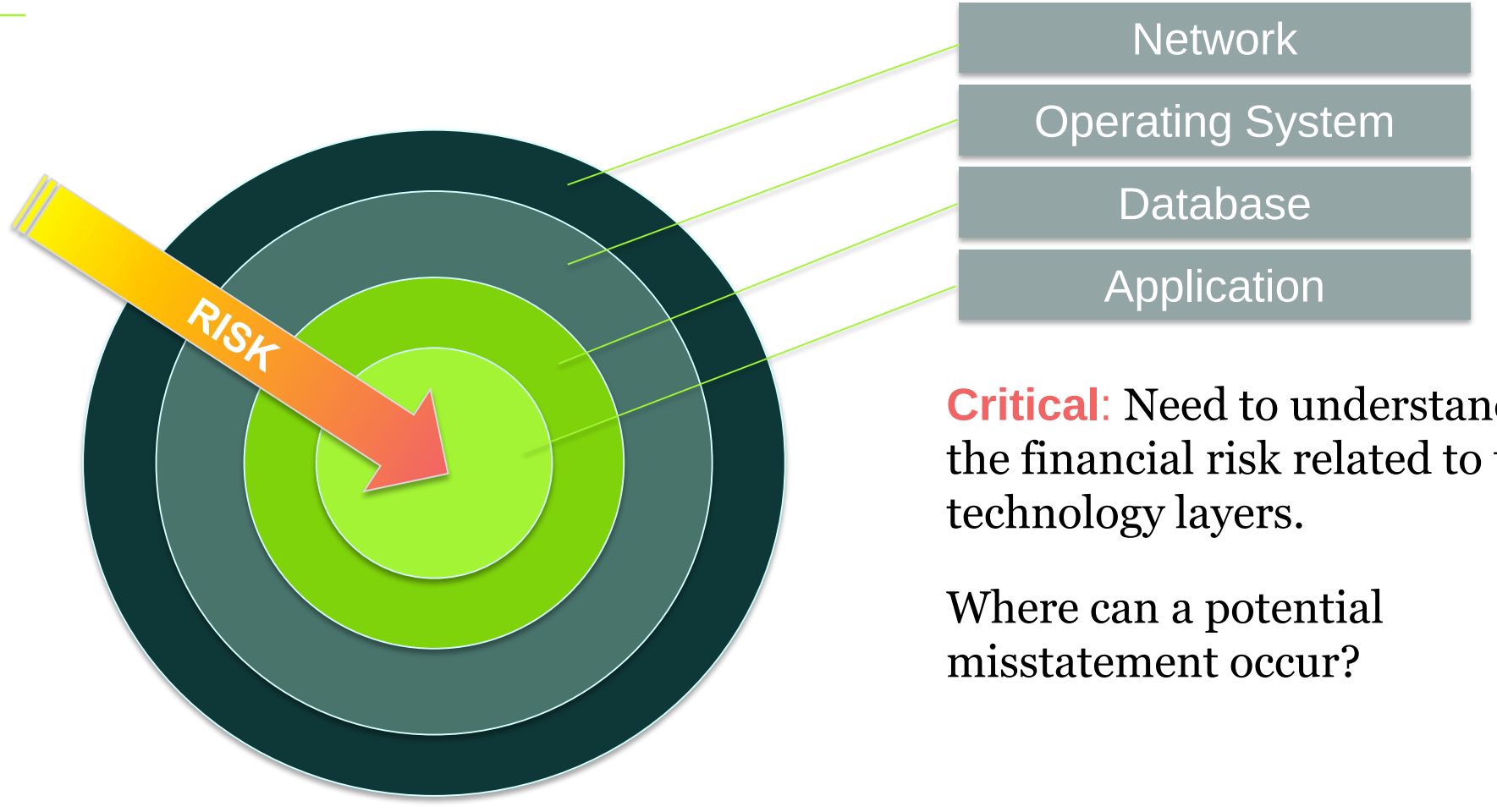
- Extensive use of technology
- Integration and knowledge
- Key reports
- Rely on automated or application controls
- Assumption that the system is always right
- Reliance on the integrity of data and information
- Efficient and effective production of financial statements

Why is IT Important?



What Are the IT Risks?

Evaluating IT Risk

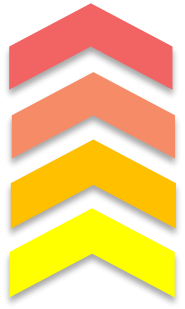


Critical: Need to understand the financial risk related to the technology layers.

Where can a potential misstatement occur?

What are ITGCs?

- Controls over applications, databases, and infrastructure components that ensure:
  - Changes are made and authorized
  - All levels of security are properly authorized and restricted
  - Systems are monitored for processing errors and to ensure information can be recovered in the event of failures
- Four domains include:
  - Systems Development Life Cycle (SDLC)
  - Change Management
  - Security
  - Computer Operations



Degree of Importance to the Financial Audit

IT General Overview – System Development (SDLC)

	When do SDLC controls apply?	What are the most important considerations for the financial statements?

SDLC	• New systems implementations
	• Major upgrades to existing systems
	• Transition to a different system
		• User acceptance testing
		  ○ Functionality: transaction processing
		  ○ Reports: financial reports and control reports
		• Data conversion/migration
		• Go-live approval

SDLC Risks

What could go wrong?

- Fictitious master data (e.g., vendors, payroll, etc.)
- Incomplete chart of accounts
- Improper classification
- Inaccurate data and balance
- Fraud
- Unknown access or conflicts
- Broken transactions

IT General Overview – Change Management

CHANGE MANAGEMENT

When do change management controls apply?	What are the most important considerations for the financial statements?

Anytime modifications are made to existing technology
• Patches and minor upgrades
• Transaction processing programs and configurations
• Interfaces
• Reports
	• Segregation of developer and production access
	• User acceptance testing
	  ○ Functionality: transaction processing, data capture, and configuration
	  ○ Reports: financial reports and control reports
	• Approval to move to production
	• Reliable tracking/documentation of changes

Change Management Risks

What could go wrong?

- Inability to rely on reports or information
- Improper classification
- Inaccurate data and balance
- Fraud
- Broken transactions

IT General Overview — Security

	When do security controls apply?	What are the most important considerations for the financial statements?
SECURITY	**ALWAYS** for financially significant applications • Not all users are created equal (e.g., read-only, write) • Superusers	• Restricted/segregated administrative access • Restricted superuser access • Segregation of duties for business users • Auditing/monitoring of superuser or sensitive access • Reliable tracking/documentation of user administration activities

Security Risks

What could go wrong?

- Improper separation of responsibilities
- Manual and mitigating controls performed by the same person
- Inability to rely on application data
- Inaccurate data and balance
- Fraud
- Management override

IT General Overview – Computer Operations

COMPUTER OPERATIONS

When do computer operation controls apply?	What are the most important considerations for the financial statements?
ALWAYS for any financially significant application • Varying degrees of risk depending on the relative impact to financial data	• Batch processing of transaction data within an application • Interfaces between applications • System issues leading to downtime • Lost data • Review of third-party service providers (SOC report review)

Operations Risks

What could go wrong?

- Improper interfaces
- Missing or incomplete data
- Inability to restore information
- Overridden or lost data/information

Application Controls

Types of Controls

YES	**Inherent:** Delivered with the application; cannot be modified
	Configuration: Customizable based on business needs and requirements; defined by management
	Calculation: Mathematically determined complex or large volume transactions based upon a predefined formula; may also be a configuration
	Validation Checks: Ensure data accuracy upon input
	Workflow: Procedures or processes created to ensure the proper routing of a transaction; requires configuration of routing rules
YES	**Security:** Determines what a user can do in the system; restricted access, roles and responsibilities, and/or segregation of duties

Key Reports

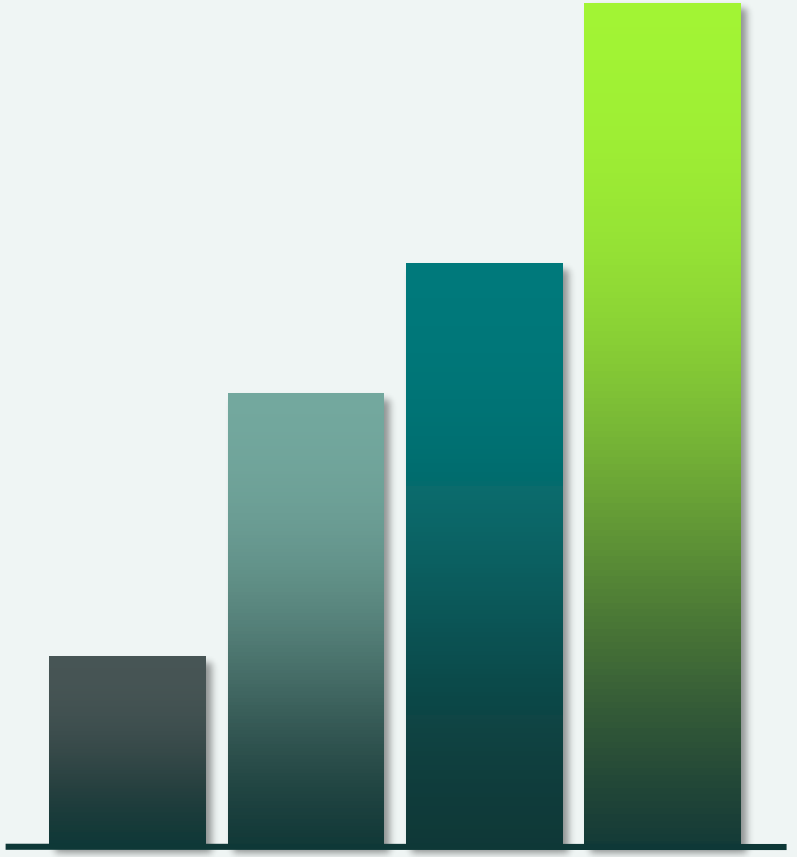
What Are Key Reports?

Financial Reports

- Income Statement
- Balance Sheet
- Revenue by Country

Control Reports

- AR Aging
- Asset Register
- JE Listing



Key Reports – Type of Report

High < Testing Difficulty > Low

Standard/Canned	Delivered with the application; not modifiable without vendor support ✓ Subject to formal ITGCs
Custom	Developed by management; customizable format and content ✓ May be in the application or a reporting tool ✓ Likely subject to formal ITGCs
Query/Ad hoc	Developed by management on an as-needed basis; customizable format and content ✓ May be in the application or a query/reporting tool ✓ Not usually subject to formal ITGCs

Key Reports

- Important to understand the nature of the report, which influences the degree of difficulty and approach for validating the report
- Completeness and accuracy considerations
  - Information prepared by the entity (IPE)
  - Are ITGCs effective?
  - What independent/reliable sources can the report be tied to?

How Should Accounting and Finance Personnel Be Involved in IT?

How Should Accounting and Finance Personnel Be Involved in IT?

System Development

- Development of requirements
- Evaluation of products
- User acceptance testing
- Evaluating data conversion

Change Management

- User acceptance testing
- Functionality: transaction processing, data capture, and configuration
- Financial reports

How Should Accounting and Finance Personnel Be Involved in IT?

Security and Access

- Approval of access
- Periodic review of user access
- Segregation of duties

Computer Operations

- Review of third-party SOC reports
- Knowing if your data could be restored in the case of loss
- Monitoring of batch processing

MOSSADAMS

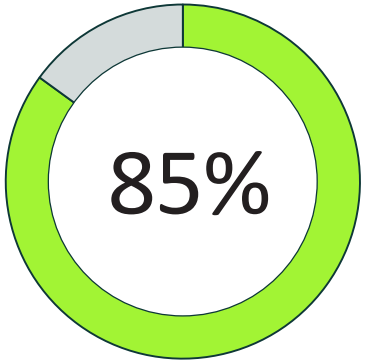
The State of Cybersecurity

State of Cybersecurity Today

It's no longer a question of whether a network will be compromised, but when a network will be compromised.

COMPANIES
that experienced at least one security incident

Source: 2017/18 Kroll Annual Global Fraud and Risk Report



7.8+ billion

Total number of records lost or stolen.

Source: 2017 Year End Data Breach QuickView Report by Risk Based Security

$3.62 million

Average cost a company pays for a data breach.

Source: 2017 Cost of a Data Breach Study - Ponemon Institute

$2 trillion

Total cost of data breaches and cybercrime worldwide by 2019.

Source: 2016 Verizon Data Breach Investigations Report

Why the Surge of Attacks?

- Attackers are more sophisticated, better funded, and attacks are multifaceted
- More resources at an attacker's disposal
- Social engineering attacks
  - Phishing/Spearphishing
  - Phone-based impersonation
- Why hack a system (lower probability) when you can hack people?
- More ingress points to the network, including mobile devices
- Ransomware = easy money!

Types of Sensitive Data

Personally Identifiable Information (PII): Any data that could potentially identify a specific individual.

Cardholder Data: Data associated with payment cards such as primary account numbers, card verification values (CVV), or track 1 & 2 data.

Protected Health Information (PHI): Individually identifiable health information that can be linked to a particular person. Protected by HIPAA.

Proprietary Information (PI): Information an organization wishes to keep confidential.

The Going Price of Your Data

SOCIAL SECURITY NUMBER
including name

CREDIT CARD
low-end includes number, type, expiration date, CCV number, and account holder's name, while the high-end includes the SSN, address, and DOB

DRIVERS LICENSE

ONLINE PAYMENT SERVICES (PAYPAL)

MEDICAL RECORD
including SSN, banking details, demographic, and job details

*Depends on how complete they are as well as if it's a single record or an entire database.

Source: 2017 study by Experian

City of Atlanta – Recent Data Breach Example

- On March 22, 2018, five of 13 municipal departments were hit with a ransomware attack
- Utility billing, public works, court, and HR systems were impacted
- Ransom was set at $51,000 in bitcoin, which the city has not paid
- SamSam variant ransomware was used – first identified in 2015
- The city had only begun to address multiple severe vulnerabilities identified during an IT security audit
- $2.7 million paid thus far to recover systems, which were down for almost a week
- Final cost could be around $17 million according to *Atlanta-Journal Constitution*

Other Municipal Cyberattacks

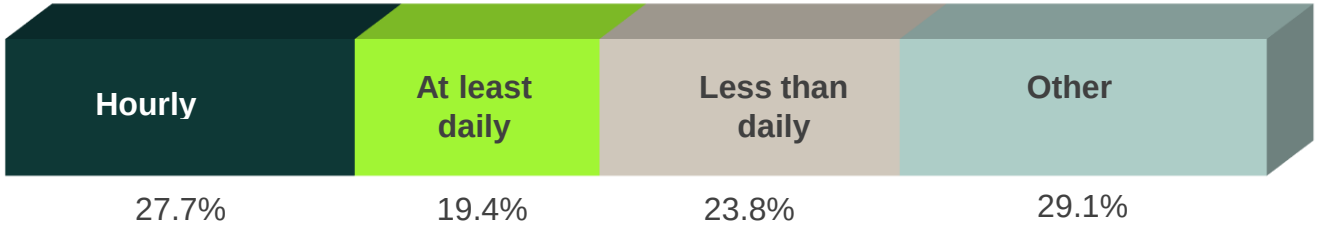
City of Baltimore	City of Fort Worth
• Late March 2018—within one-week of Atlanta attack • 311 and 911 computer-aided dispatch systems offline for more than 17 hours • System taken offline and rebuilt • Cause: Firewall change with inbound port left open for about 24 hours	• January through March 2018 automated bot-based attacks • 17 million attempts to crack passwords;, 700,000 attacks against servers and email • Possibly state sponsored • Blocked 3,260 spyware and 1,350 virus downloads

Local Governments in Cyber Peril

- International City/County Management Association (ICMA) survey from 2016 (reported in *The Conversation*)
- Sent to 3,423 US local governments with populations over 25,000
- 411 responded (267 cities and 144 counties)

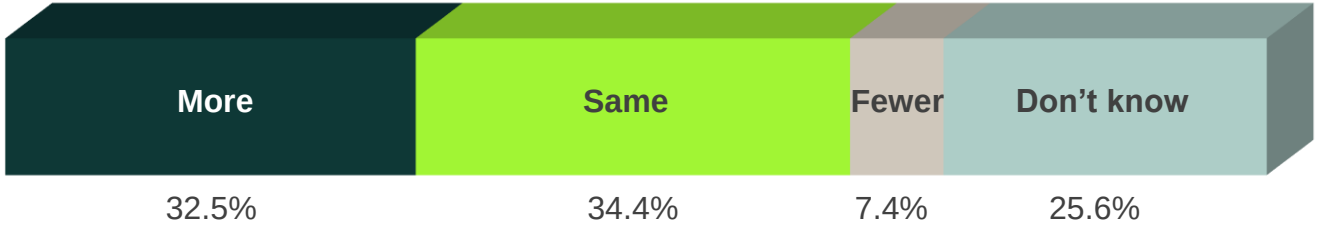
Local Governments in Cyber Peril

How frequently is your local government under attack?



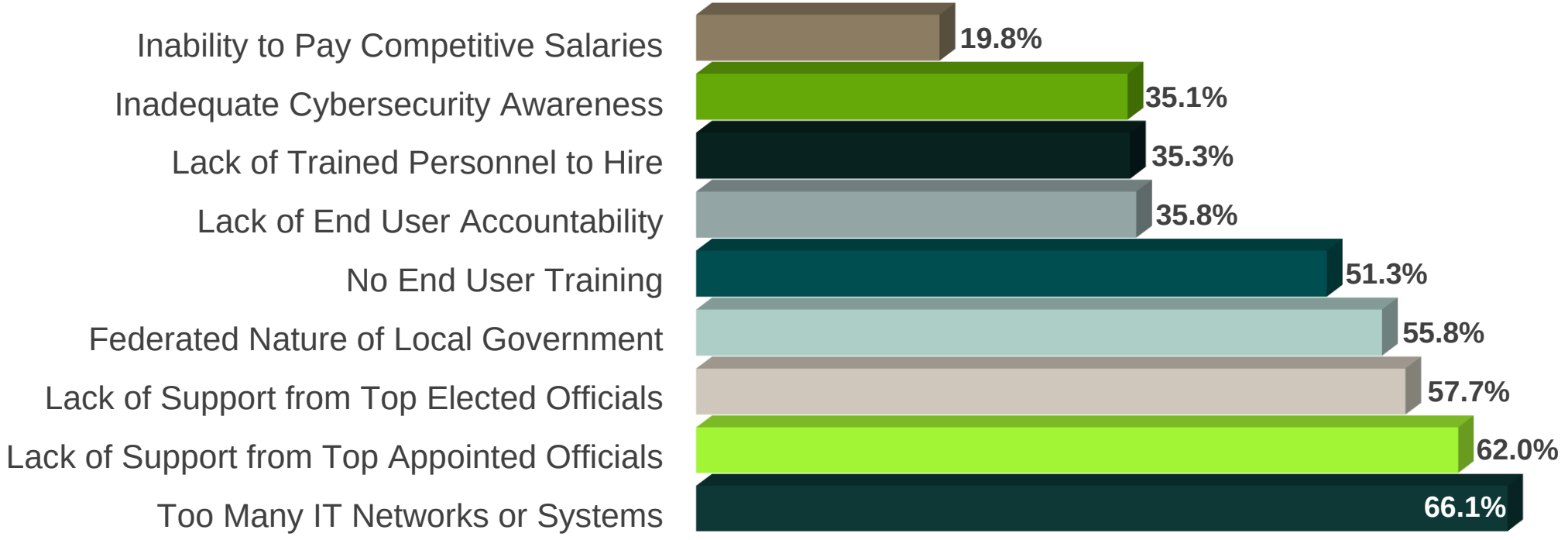
How aware are top-appointed managers of the need for cybersecurity?

How many cyberattacks did you experience this year compared to last?



Local Governments in Cyber Peril

Which of the below barriers severely impede your local government's cybersecurity?



Top Cybersecurity Threats

Common Cyberattacks

Spearphishing

An email that asks for information—login credentials or bank details—in the hopes of someone innocently responding and providing it.

CEO Fraud/Whaling

This method is the same as spearphishing but targets C-level executives.

Ransomware

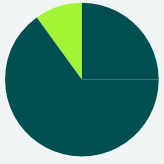
Hackers gain access to a system using malicious software, then encrypt sensitive data and hold it hostage—along with your ability to conduct business—until a demand is satisfied.

Malicious Code and Malware

These are programs such as viruses, trojans, worms, and others that disrupt normal computing to exploit system security flaws.

The Internet of Things (IoT)

Another entry point to hackers



90%
of consumer products will have the ability to interact with other devices in 2017

Source: Samsung

26–50 billion
IoT devices will be connected by 2020

Source: Gartner and Cisco, respectively

Per the IoT Consortium and NIST Industrial IoT Framework, devices that depend on the IoT are particularly vulnerable as vendors are rushing to get products out in the marketplace without considering security elements. Examples of this include:

- AVL sensors in public transit cards
- Smart video conferencing systems
- RFID inventory systems
- Vending machines
- Fitbits and smart watches
- Wireless HVAC systems
- Medical devices

Characteristics: limited processing power, sensor triggers, actuators, “machine-to-machine” communication

Cryptomining Attacks

- Became the biggest threat starting in 2018, ahead of ransomware
- Attackers hijack systems to mine digital currencies, also known as drive-by cryptomining
- Cryptocurrency-mining malware provides a stealthier, more effective alternative to ransomware
- Trend Micro detected 141 percent increase in cryptojacking attempts, along with 47 new cryptocurrency miner malware families in the first six months of 2018
- WannaMine – derivative of WannaCry

S3 Misconfigurations

- Misconfigured Amazon Simple Storage Service (S3) buckets allow man-in-the-middle (MitM) attacks
- Misconfigurations leave the data vulnerable to attackers
- Fix is easy and Amazon has material on how to set the correct permissions

Organization	Number of Records Exposed	Type of Information Exposed
LocalBlox	48 million	Names, physical addresses, birthdates, Twitter handles
LA County 211	3.2 million	Names, email addresses, and encrypted passwords
Alteryx	120 million	Personal information, including demographics and finances

Are You Prepared for a Cyberattack or Breach Attempt?

What is Red Team Penetration Testing?

- A test of your organization's ability to respond to a real-world cyberattack
- A way of measuring how effective your incident response procedures are
- An opportunity to get fresh eyes and advice on how to improve your incident response procedures

What Red Team Penetration Testing is Not

- A test of only one variable (such as firewalls, a specific web application, or your people)
- A Same-as-Last-Year assessment
- A “vulnerability assessment scan” or “network penetration test”

Offensive Security Assessments

FOCUS AREAS	External Vulnerability Assessment	Network Penetration Test	Social Engineering Assessment	Internal Vulnerability Assessment	Internal Penetration Test	Red Team Penetration Test
Security operations center/ incident response team						X
Antivirus/antimalware					X	X
Host-based hardening				X	X	X
Network hardening				X	X	X
Internal network segmentation				X	X	X
Employee awareness			X			X
Physical security procedures			X			X
Antispam/email filter		X	X			X
Network IDS/IPS		X				X
Network firewall	X	X				X
Web application firewall	X	X				X
Network Monitoring	X	X		X	X	X

Expected Benefits

- Gain the perspective of a consultant who is familiar with your industry, market segment, and business model
- Validate existing controls and provide support for timelines (SLAs)
- Provide evidence of regulatory compliance (PCI, HIPAA, FFIEC, NIST/DFARS, etc.)

When is This Testing Most Beneficial?

- After key personnel changes (CISO, CTO, Director of IT, etc.)
- After social engineering awareness training or information security training
- When preparing for an audit or visit from regulators
- To test a major upgrade, rollout, or infrastructure change
- On a regular annual or semiannual basis

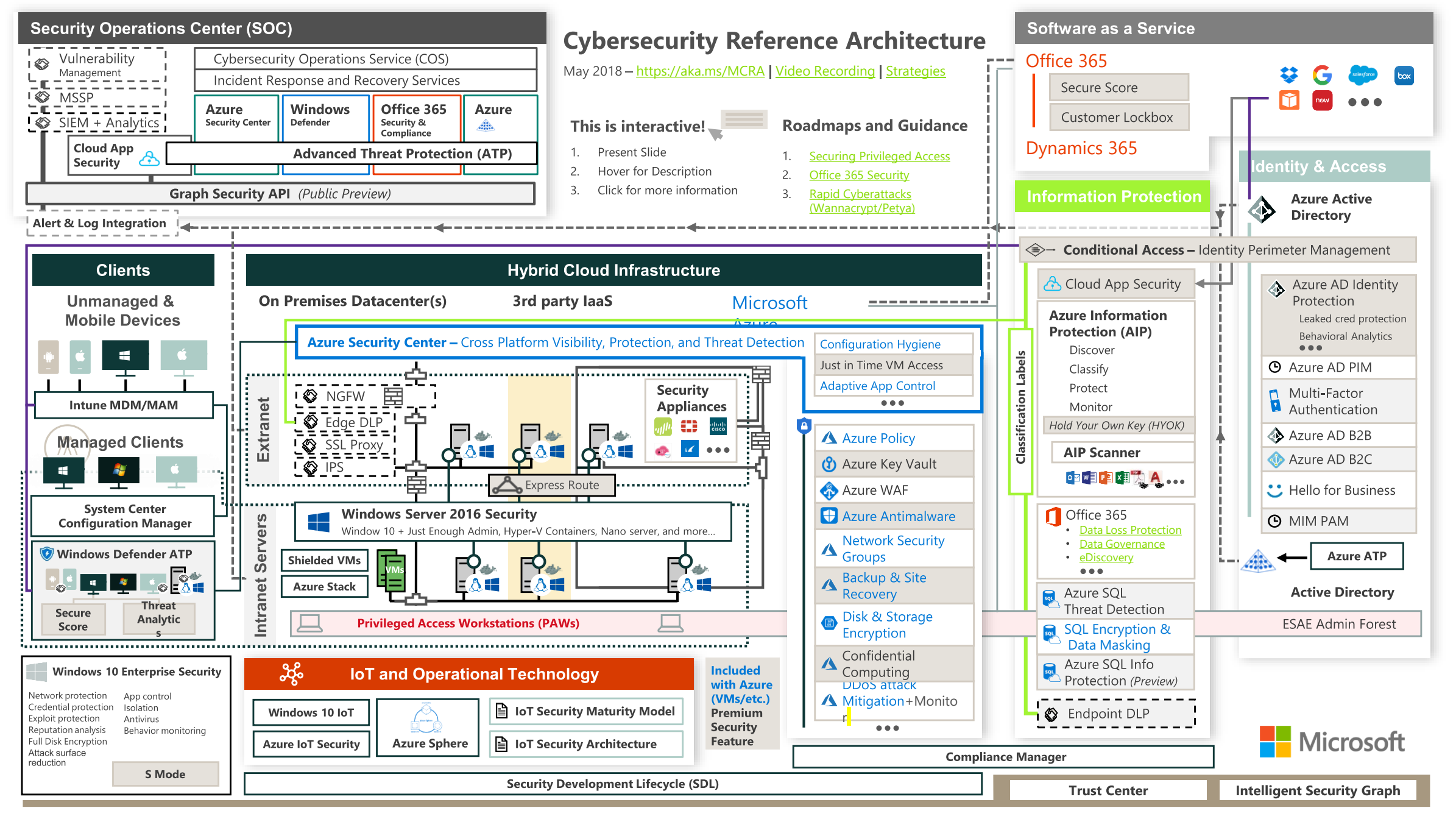
Pros & Cons

PROS

- More advanced and customized than traditional penetration testing
- Provides a better indication of actual security posture by developing a real-world scenario
- Leads to more specific and right-sized recommendations on how to improve security controls
- Measures the effectiveness of incident response programs

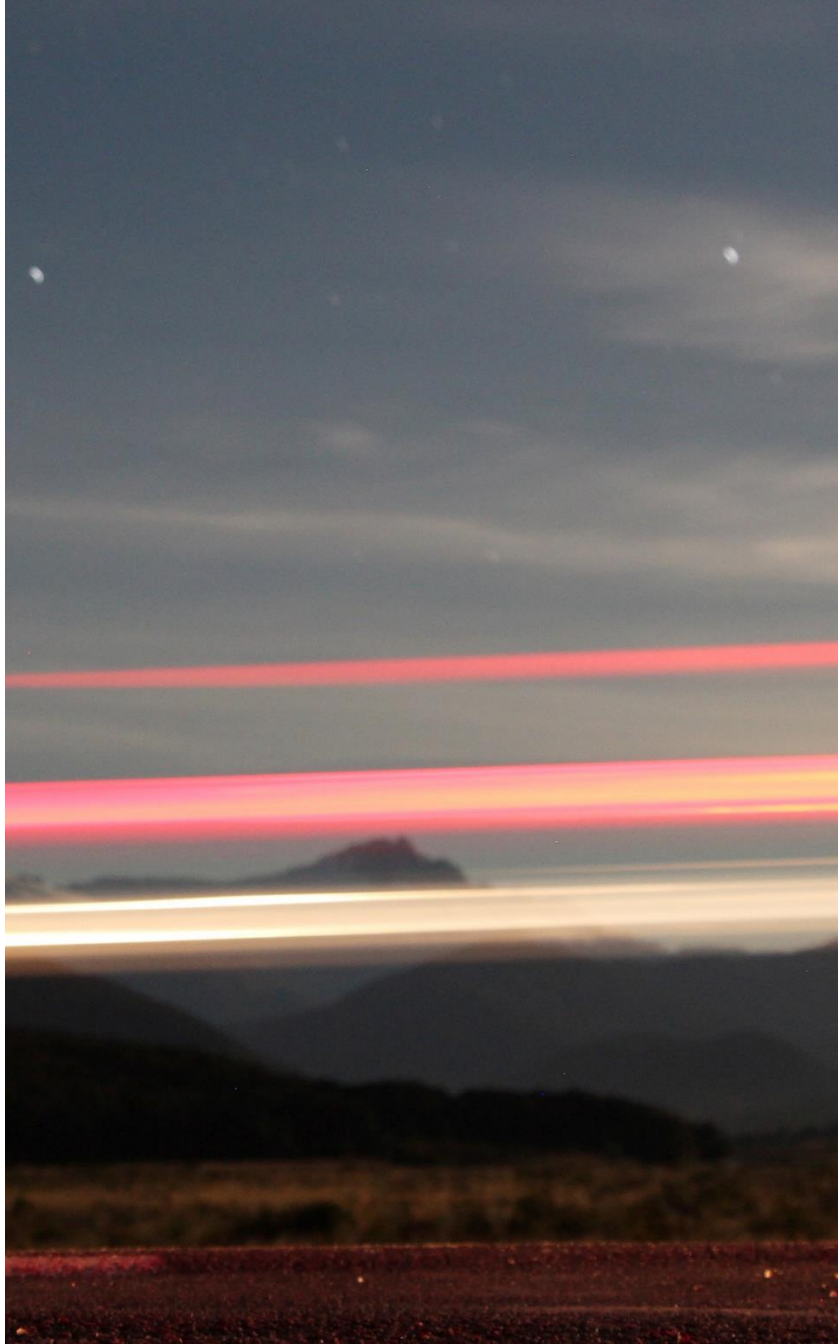
CONS

- Higher cost than traditional penetration testing
- Must be performed by a trusted advisor—be wary of unsolicited service offers
- Often takes longer and requires more preparation than a traditional vulnerability assessment or penetration test
- Fewer providers may lead to fewer options to select from


Security Operations Center (SOC)
Vulnerability Management
MSSP
SIEM + Analytics
Cybersecurity Operations Service (COS)
Incident Response and Recovery Services
Azure Security Center
Windows Defender
Office 365 Security & Compliance
Azure
Cloud App Security
Advanced Threat Protection (ATP)
Graph Security API (Public Preview)
Alert & Log Integration
Cybersecurity Reference Architecture
May 2018 – https://aka.ms/MCRA | Video Recording | Strategies
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Roadmaps and Guidance
1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)
Software as a Service
Office 365
Secure Score
Customer Lockbox
Dynamics 365
Identity & Access
Azure Active Directory
Information Protection
Conditional Access – Identity Perimeter Management
Clients
Unmanaged & Mobile Devices
Intune MDM/MAM
Managed Clients
System Center Configuration Manager
Windows Defender ATP
Secure Score
Threat Analytics
Hybrid Cloud Infrastructure
On Premises Datacenter(s)
3rd party IaaS
Microsoft Azure
Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection
Configuration Hygiene
Just in Time VM Access
Adaptive App Control
Extranet
NGFW
Edge DLP
SSL Proxy
IPS
Express Route
Security Appliances
Intranet Servers
Windows Server 2016 Security
Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
Shielded VMs
Azure Stack
VMs
Privileged Access Workstations (PAWs)
Azure Policy
Azure Key Vault
Azure WAF
Azure Antimalware
Network Security Groups
Backup & Site Recovery
Disk & Storage Encryption
Confidential Computing
DDoS attack Mitigation+Monitor
Classification Labels
Cloud App Security
Azure Information Protection (AIP)
Discover
Classify
Protect
Monitor
Hold Your Own Key (HYOK)
AIP Scanner
Office 365
Data Loss Protection
Data Governance
eDiscovery
Azure SQL Threat Detection
SQL Encryption & Data Masking
Azure SQL Info Protection (Preview)
Endpoint DLP
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Multi-Factor Authentication
Azure AD B2B
Azure AD B2C
Hello for Business
MIM PAM
Azure ATP
Active Directory
ESAE Admin Forest
Windows 10 Enterprise Security
Network protection
Credential protection
Exploit protection
Reputation analysis
Full Disk Encryption
Attack surface reduction
App control
Isolation
Antivirus
Behavior monitoring
S Mode
IoT and Operational Technology
Windows 10 IoT
Azure IoT Security
Azure Sphere
IoT Security Maturity Model
IoT Security Architecture
Included with Azure (VMs/etc.) Premium Security Feature
Compliance Manager
Security Development Lifecycle (SDL)
Trust Center
Intelligent Security Graph
Microsoft

Takeaways

- Attacks will continue to evolve in sophistication
- Municipalities and county governments remain vulnerable
- Cryptomining/cryptojacking, IoT, and cloud-based misconfigurations serve as new attack vectors for cybercriminals
- Red Team Penetration Testing is a way to truly test your defenses and incident response strategy



The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.

THANK YOU

Questions?

Before You Go...

More Moss Adams Insights and Resources are a click away

Visit our website to find:

- More on-demand webcasts
- General and industry-specific newsletters, articles, and alerts
- RSS feeds
- Connect with us – subscribe to Moss Adams content

Contact

Colin Wallace, Partner

(972) 924-5089
colin.wallace@mossadams.com

Francis Tam, Partner

(310) 295-3852
francis.tam@mossadams.com