Cybersecurity

Metropolitan Washington Council of Governments
BOARD OF DIRECTORS

Wanda M. Gibson
Chief Information Officers Committee Chair - Fairfax County CTO

Michael T. Dent
Chief Information Security Officers Committee Chair - Fairfax County CISO

March 13, 2019

NATIONAL CAPITAL REGION • DC • MD • VA • HOMELAND SECURITY •

Cybersecurity

- Governments and the community are **reliant on technology and the Internet**, thus, extremely vulnerable to cyber threats such as malware, system breaches, data and identity theft, etc.
- Must have adequate **controls** and **governance** that includes security architecture, standards, **policy**, awareness, risk assessments, and **enforcement.**

Given continuous updated controls in place, some cyber attacks can be mitigated and responded to immediately.

However some breaches such as **Advanced Persistent Threats** (APT) are not immediately detectable. It can take days, weeks, and even months to detect, isolate, and mitigate and formulate a response.

Cyber Attack Ramifications

- Disruption of government services
- Compromise critical first responder services
- Destruction or alteration of records government is steward of
- Increased litigation, fines, and penalties
- Cause financial damage - negatively impact financial ratings and law suits
- Harm Reputation / Loss of Public Trust
- Harm citizens and businesses

Recent Cyber Events

October 2016: Personal data of 57M Uber drivers and riders compromised.

May 2017: Equifax breached and has 145M accounts compromised – 45% of US population

June 2017: Name, mobile number, and PIN for 14M Verizon customers posted online in unsecure area by third party vendor

March 2018: Hackers indicted for spearphishing in obtaining 31 terabytes of data worth $3B in intellectual capital from universities, private companies, including United Nations, states of Hawaii and Indiana, and the US Federal Energy Regulatory Commission

Recent Cyber Incidents

- Jackson County, GA paid $400K ransom to restore access to data on servers and workstations. FBI was leveraged to assist in investigation:

  https://www.onlineathens.com/news/20190308/cyber-attack-forces-jackson-county-to-pay-400k-ransom

- Citrix incident: Used password spraying to exploit weak passwords. Bypassed two factor security. Escalated access over time to download business documents:

  https://www.zdnet.com/article/citrix-discloses-security-breach-of-internal-network/

- 1.4 million patient records breached in UnityPoint Health phishing attack - This is the second breach for the health system this year, and the biggest health data breach of 2018 in the U.S.

  https://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack

Government & Citizen Cyber Events

Local and state governments have been victims of malware or ransomware leading to impacting certain capabilities:

- Impact to Virginia State Police (April 2017)
- Publicly exposed voter data (June 2017) by Deep Root Analytics. It is unknown who or how many times this data was downloaded prior to discovery by security researcher.

Cyber Threats – How & Why

Malware / DOS through:

- Phishing and other social engineering
- Internal threats
- Hacktivism
- Cybercrime / Cyberterrorism
- Internet spiders and BOTS - WEBSite
- Wireless devices / WiFi
- Supply Chain
- Non-compliant or misconfigured systems
- Unauthorized Cloud Usage
- WEB apps
- Downloading Subscription Services

Data Loss

Data altered

Systems disabled /unavailability to function

Misdirecting actions

Systems destroyed

Top Security Threats

Ransomware still on the rise!

-Cyber Criminals do it for the Money!

-Easily accessible now as a Service

Phishing Attacks Continue to Dominate!

- Email #1 Source
- Very Crafty in 2018

Human Factor still a weakness!

- Employees victims to Phishing
- Not thinking before clicking!

“Four percent of people will click on any given phishing campaign” - Tin Zaw, Verizon Director of Security Solutions

Distributed Denial of Service

- Causes Disruption
- Misdirection tactic by hackers

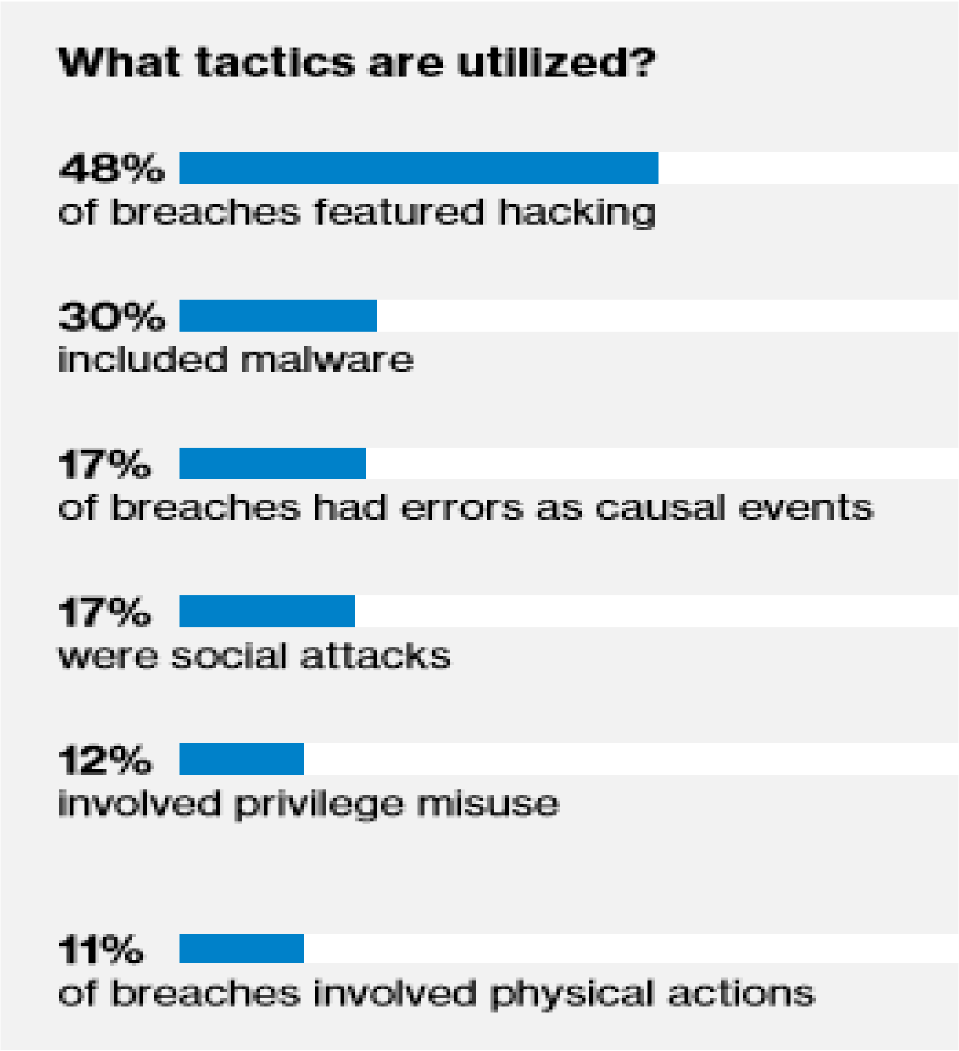
Email

- Most common source of Malware

Stolen Credentials

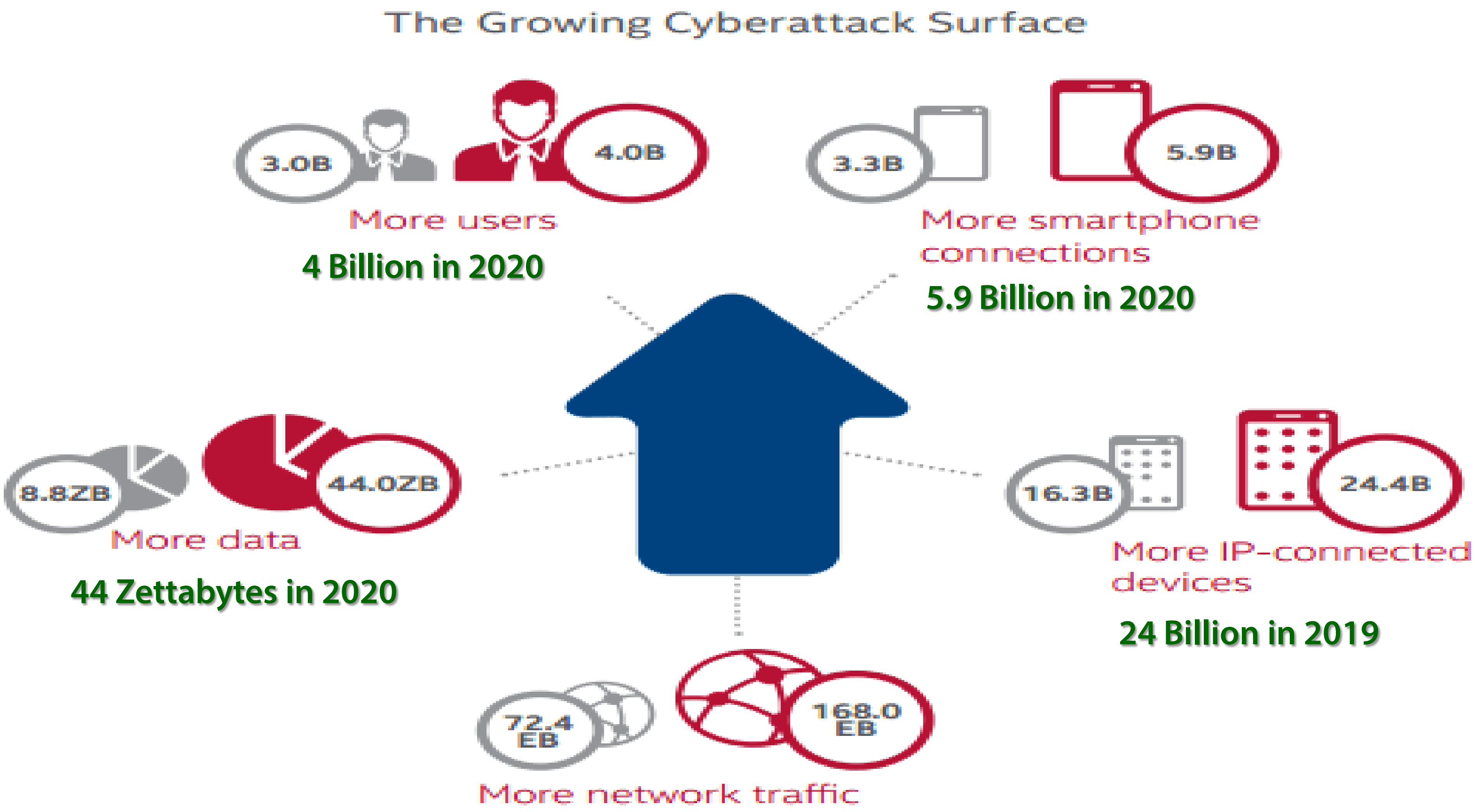
- Brute Force logins
- Lack of Multi-factor Authentication

Evolving Challenges: Industry Metrics



Source: 2018 Verizon Data Breach Investigations Report, 11th Edition.

Evolving Challenges: Industry Metrics



4 Billion in 2020

5.9 Billion in 2020

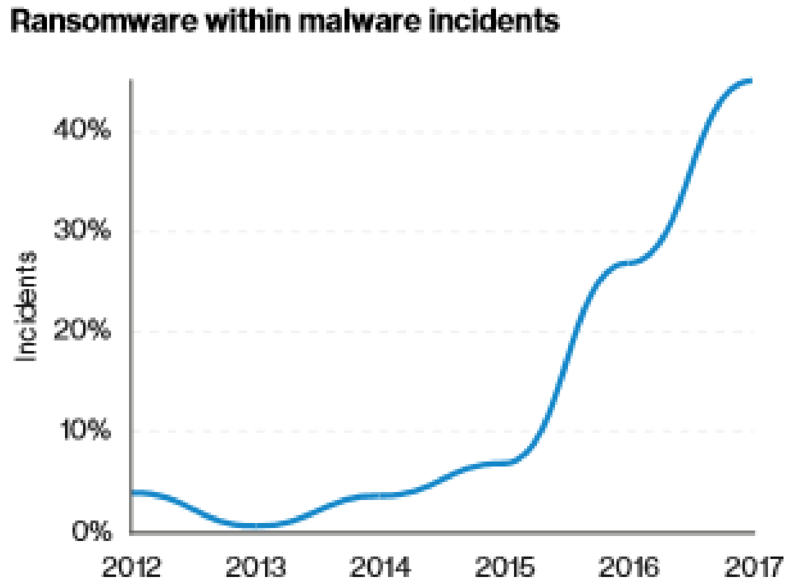
44 Zettabytes in 2020

24 Billion in 2019

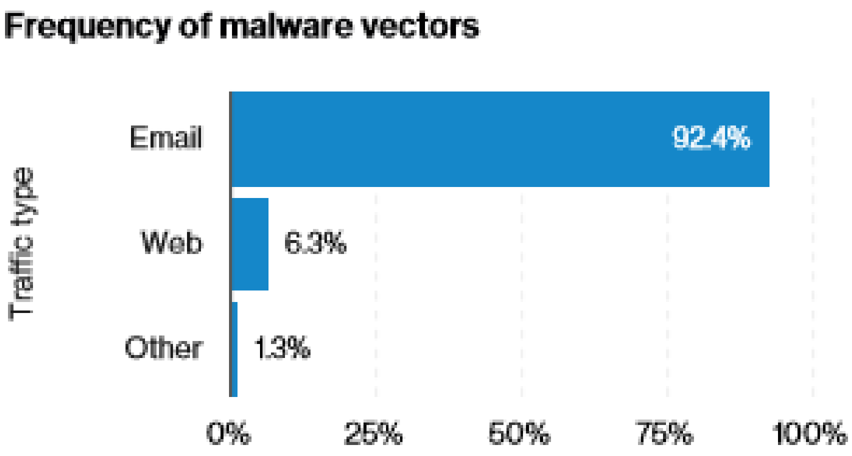
168 Exabytes per month in IP traffic in 2019

Source: McAfee Labs 2016 Threat Predictions Report.

Evolving Cybersecurity Challenges



Ransomware within malware incidents



Frequency of malware vectors

Source: 2018 Verizon Data Breach Investigations Report, 11th Edition.

ISO continue to adjust to new evolving threats through the deployment of emerging technologies:

Next-generation application-layer firewalls that offer deep-inspection of network traffic and analyze applications beyond the capabilities of traditional firewalls.

Security information and Event Management (SIEM) system to enable continuous monitoring and the correlation of network and user activity events as part of incident analysis and response.

Continuous investment is an absolute requirement

Critical Infrastructure

CIP is a rich target for cyber crime and of significant concern as Industrial Support Systems become automated and managed through the Internet

A cyber attack against a **Critical Infrastructure Provider (CIP)** sector could cause widespread chaos and panic if the attack brings down one of the following for any amount of time:

- Communications (landline and wireless)
- Energy (development and distribution)
- Food and Agriculture
- Government Facilities
- Healthcare
- Transportation Systems
- Fresh Water and Wastewater Systems

New Normal!
Coordination w/ Emergency Management tapping CISO expertise with CIPs is imperative.

On-going Regional Cyber Efforts

Chief Information Officers Committee (CIO) & Chief Information Security Officers Committee (CISO) collaboration:

- Continuously meet since 2007 on a monthly basis.
  - Establishes tech and security standards and practices
  - Collaboration, inquiries, concerns, active threats, and certain information from fusion centers

- NCR Security Management Program
  - A set of policies concerned with information management or IT related risks for region based network and apps
  - Manages information security for shared services and data functions
  - Created a regionally adopted Security Policy in 2007 aligning with the NIST Cyber (updated in 2010, and 2013)
  - Mutual Aid

Regional Cyber Efforts

- Developed and maintained the Cybersecurity Annex to the Regional Emergency Coordination Plan (RECP) from both a jurisdictional and regional perspective

- Cybersecurity is Regional Priority for 2018 over next three years
    - Consists of defined priority statement and outcomes to improve cybersecurity posture

- Cyber Working Group formed in November 2018
    - Regional Cybersecurity Coordinator position funded

Regional Cyber Capabilities

- Identity Access Management System (IAMS)
  - Allows end users to utilize their existing, jurisdictionally-issued username and password to access regional applications.

- National Capital Region Network (NCRnet)
  - Locality Interconnect protected from external access
  - Uses the latest network technology allows for separation, security, and prioritization of network traffic for different categories of applications and data
  - Operates intrusion detection and prevention services

Local Undertakings

Some of the localities use the **National Institute of Standards and Technology (NIST) Cybersecurity Framework**, a federal best practices guide and security policy framework

Imperative to-do: Develop a Security Management Program:

- Assign a dedicated and **qualified CISO**.
- **Empower the CISO** with executive leadership support for the CISO to work with the agencies.
- Establish and maintain an **IT Security Policy** with teeth *and* an associated **No Tolerance HR Policy**
- Subscribe to **MS-ISAC and/or other CERTS**
- Obtain **Cyber Insurance**
- Perform **Risk Assessments** on a routine basis.
- Instill **Security Awareness** training as part of an employee's onboarding, and periodic re-certification.
- **Establish investment plan** for protective measures as business foundational capability.
- **Monitor & Audit**

Cybersecurity Goals

- Invest in IT security architecture and tools, monitoring, and compliance
- Coordination with law enforcement
- Establish integration with Critical Infrastructure Protection (CIP) assets
- Establish Cyber Awareness & Training
- Establish Standard Operations Procedures (SOP) and communications protocols
- Establish Security Operations Center (SOC)

Get Cyber Insurance

Regional Cyber Goals

Reality Check

- Continuity of Operations Plan (COOP)
  - Do you know where it is located?
  - Does it contain a cyber security scenario?
  - Based on evolving cyber threats, how often is it updated?

- Exercise your COOP:
  - How frequently do you exercise your plan?
  - Determine citizen impacts
  - Exercise the plan with your Information Technology team, from the inside out

Cybersecurity Goals

- Investment in Cyber Security should allow for continuous updating.
  - Technology
  - People
  - Process

- Include cyber security and privacy requirements in **all services and products contracts.**

- Update **contracts** for CIP providers that include accountability for cyber response

- Develop strategic plan to refresh IT infrastructure in line with best practices (Cyber Security Threat protection is only as strong as the weakest link.. e.g.: Windows XP)

National Cybersecurity Awareness

October is National Cybersecurity Awareness Month

- COG has an annual Cybersecurity awareness conference
- Fairfax County holds cybersecurity conference for county and regional employees
- D.C. has hosted cyber security awareness events
- NACO sponsors cyber security conference platform
- Elected officials across NCR have declared October as Cyber Security Month in their localities

Questions?

Resources

National Cyber Security Awareness Materials

https://www.dhs.gov/national-cyber-security-awareness-month

https://www.cisecurity.org/ms-isac/ms-isac-toolkit/

https://staysafeonline.org/data-privacy-day/get-involved/

https://www.cisecurity.org/resources/daily-tip/

Cyber Security Information and Updates

https://www.nist.gov/cyberframework

https://www.cisecurity.org/ms-isac/

https://lists.sans.org/mailman/listinfo

Verizon DBIR: https://enterprise.verizon.com/resources/reports/dbir/

ID Theft Center Report: https://www.idtheftcenter.org/