



# 20th Annual Privacy and Security Conference

Looking Back and Leading Forward in a Digital World

Feb.6-8, 2019, Victoria, BC

[Register](#)

## Cybersecurity Update: Phishing to Ransomware – Looking ahead to 2019



*Kevin J. Murphy, CISSP, CISM, CGEIT*



# Agenda

A very interactive discussion – We learn from each other!

- *Who is in the room?*
- *Lessons from 2018*
- *Looking ahead to 2019*
- *Vendor verification*
- *Quick review*

# Who is in the room?

- Provincial Government
- Federal Government
- Municipal
- Retail
- Technology
- Transportation
- Law Enforcement
- Healthcare
- Energy
- Telecom
- Financial
- Manufacturing
- Education
- Services

# Who is attacking?

News > UK

**North Korea were behind NHS cyberattacks**  
**Security**  
**national revelation**



NotPetya attack is widely thought to have been carried out by Russia, an allegation Moscow denies.



The Canadian government's computer networks have been hit by state-sponsored cyberattacks about 50 times a week — and at least one of them usually succeeded.

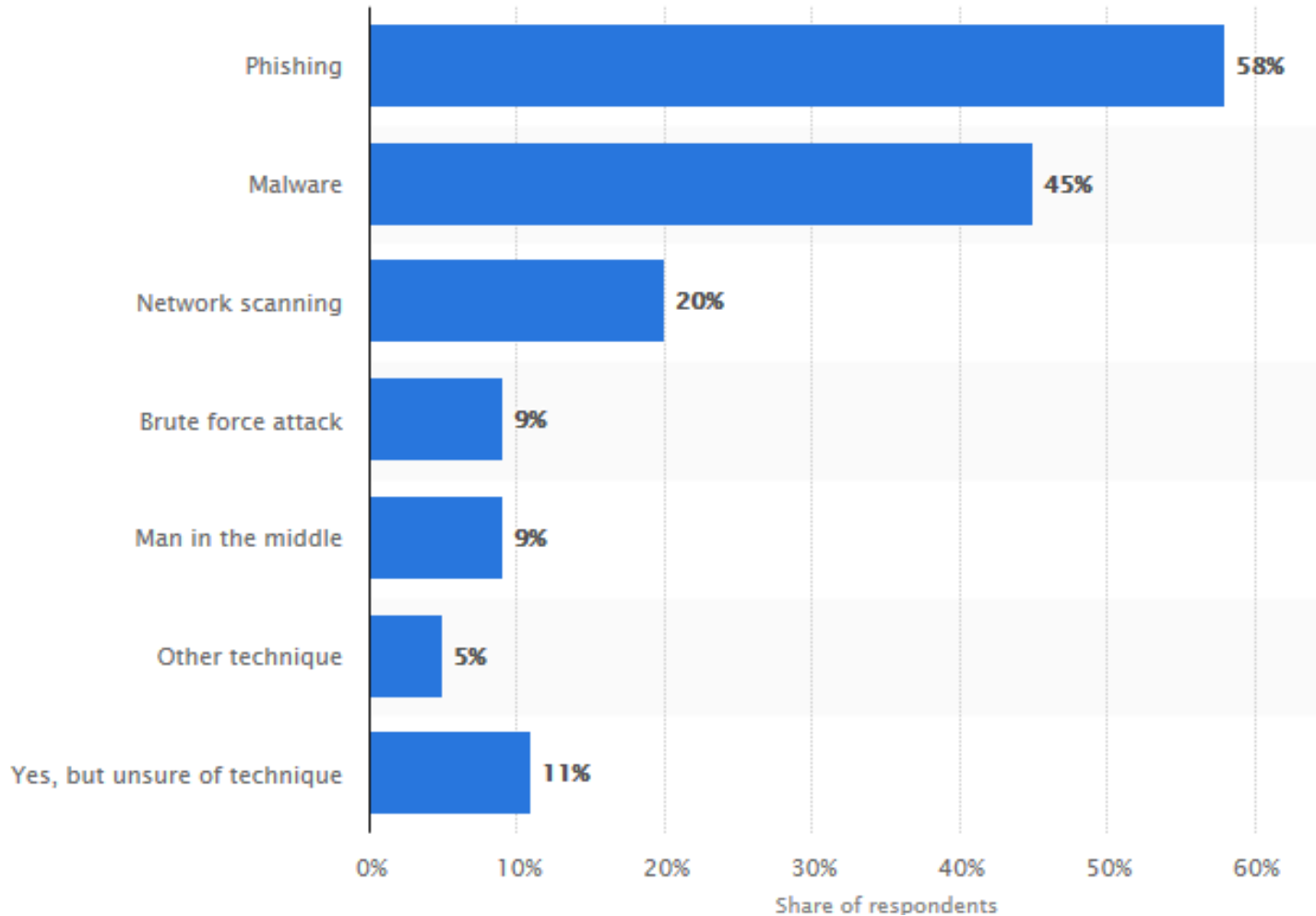


On October 24th... targets Windows... Adobe Flash... attack has seen computers go... Russia, Ukraine, Germany and Turkey.



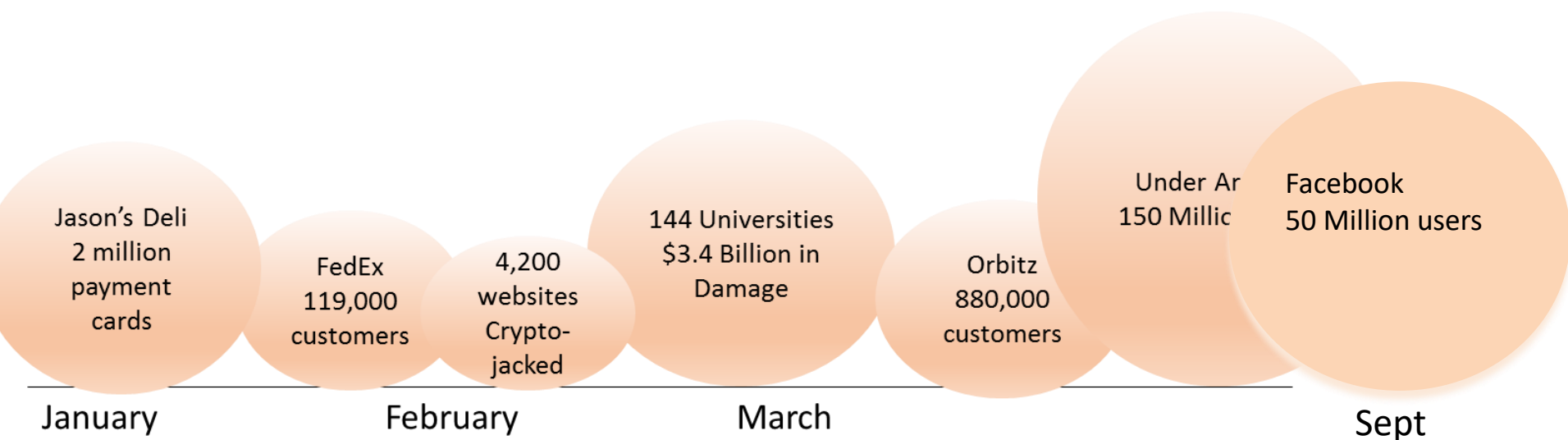
***“The new Cold War with less rules”***

# 2017 Canadian Companies



<https://www.statista.com/statistics/827317/canada-companies-cyber-attacks-techniques-used/>

# 2018 Notable Cyber Breaches



[Risk Based Security](#) in Richmond, Va. reported data as of June 30 showing the United States had, by far, the most incidents per country at 1,074. United Kingdom was second with 62 and Canada third with 48 incidents

# 2018 Reality



## CyberAttacks:

- Data breaches have hit 36 per cent of Canadian businesses.
  - <https://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/>
- **Cyber-attacks on Canadian municipalities increasing**
  - <https://auma.ca/news/cyber-attacks-canadian-municipalities-increasing>

# New Breach Regulations

- Commencing November 1, 2018, Canada's federal [Personal Information Protection and Electronic Documents Act](#) ("PIPEDA") will require an organization that suffers a "breach of security safeguards" involving personal information under its control to keep prescribed records of the breach and, if the breach presents a "real risk of significant harm to an individual", to promptly report the breach to the Privacy Commissioner and give notice of the breach to affected individuals and certain other organizations and government institutions.

- 

<https://cybersecuritylaw.ca/home/2018/4/22/canadian-personal-information-security-breach-obligations-preparing-for-compliance>

# 2018 Reality



## Malware

- Up 102% in 2018 from 2017
- Also more threats via smart malware and file-less malware
- Malware attacks on non-profits as staging areas for attacks on business
  - Youth activity, charities, social sites, the arts, etc. generally have marginal security

## Ransomware

- Up 229% in 2018 from 2017
- West Jet, City of Atlanta, Univ of Calgary, Colorado, Alaska, etc, etc.

## Attackers leveraging encryption (SSL/TLS) to bypass your security controls

- Up 275% in 2018 from 2017
- 2/3<sup>rd</sup> of City of Seattle Internet traffic is now Https
- Attackers can leverage free SSL certificates using “Let’s Encrypt” to disguise their traffic.
- Our City non-encrypted traffic now ~8% and getting smaller. **Your network traffic monitoring is blind if you are only inspecting port 80 traffic**

# Who is attacking?

Destination IP	Destination Port (Unique Count)	Source IP (Unique Count)	Source Port (Unique Count)	Event Name (UR Count)
88.214.193.180	443	Multiple (15)	Multiple (136)	Firewall Drop
136.243.73.56	443	156.74.159.228	Multiple (39)	Firewall Drop
119.28.109.132	80	156.74.90.217	Multiple (28)	Firewall Drop
5.9.7.202	443	156.74.135.245	Multiple (19)	Firewall Drop
85.195.100.210	Multiple (2)	Multiple (9)	Multiple (19)	Firewall Drop
178.62.242.42	Multiple (2)	Multiple (4)	Multiple (12)	Firewall Drop
88.99.5.37	443	Multiple (2)	Multiple (10)	Firewall Drop
85.195.104.15	443	Multiple (2)	Multiple (10)	Firewall Drop
84.22.110.176	443	10.4.162.55	Multiple (10)	Firewall Drop
213.230.210.230	443	Multiple (8)	Multiple (8)	Firewall Drop
88.214.193.110	443	Multiple (3)	Multiple (9)	Firewall Drop
149.202.194.227	Multiple (2)	Multiple (2)	Multiple (5)	Firewall Drop
149.202.212.167	443	Multiple (2)	Multiple (6)	Firewall Drop
92.63.111.166	443	156.74.84.43	Multiple (6)	Firewall Drop
178.63.70.146	443	Multiple (2)	Multiple (5)	Firewall Drop
136.243.74.163	443	156.74.26.203	Multiple (4)	Firewall Drop
51.255.231.130	443	Multiple (2)	Multiple (7)	Firewall Drop
167.114.210.7	443	172.16.102.167	Multiple (4)	Firewall Drop
194.226.130.227	443	172.16.102.232	Multiple (6)	Firewall Drop
144.217.84.97	443	156.74.187.189	Multiple (3)	Firewall Drop
77.246.156.238	443	156.74.84.43	Multiple (3)	Firewall Drop
51.255.232.205	80	156.74.186.237	Multiple (3)	Firewall Drop
148.66.136.190	80	156.74.123.29	22519	Firewall Drop
46.254.20.14	80	156.74.34.93	21817	Firewall Drop
208.91.197.132	443	156.74.20.138	Multiple (3)	Firewall Drop
88.214.193.96	80	Multiple (2)	Multiple (2)	Firewall Drop
88.214.193.9	443	Multiple (2)	Multiple (4)	Firewall Drop
194.226.130.229	443	172.16.102.232	Multiple (4)	Firewall Drop
185.53.178.7	443	156.74.149.252	Multiple (2)	Firewall Drop
31.172.81.172	443	Multiple (2)	Multiple (4)	Firewall Drop
31.172.81.160	443	Multiple (2)	Multiple (4)	Firewall Drop
31.172.81.158	443	Multiple (2)	Multiple (4)	Firewall Drop
88.214.193.33	80	156.74.68.152	23179	Firewall Drop
85.195.107.98	51700	10.5.192.190	51700	Firewall Drop
194.226.130.226	443	172.16.102.232	Multiple (2)	Firewall Drop
194.226.130.228	443	172.16.102.232	Multiple (2)	Firewall Drop
46.36.39.39	443	156.74.20.117	32029	Firewall Drop

# 2018 Reality



## Phishing

- **Employee Awareness**
  - Nearly **1.5 million phishing URLs are created each month** just to trick users into thinking an email is indeed originating from their employer, Microsoft, the CRA, their bank, Facebook page, insurance claim form, PayPal, Apple, etc.
- **Cloud Applications: e.g O365**
  - Base subscriptions has insufficient security as standalone product; think “Defense in Depth”
- **Outnumbered by Malicious Actors**
  - They are right once and win; we have to be right 100% of the time
  - And they are using AI against you.

# Quiz

- Which country hosts the most malicious web addresses?

Ranking in Q2	Country/region	Number of domains in Q2	Number of domains in Q1
1.	US United States	248	257
2.	NL Netherlands	31	13
3.	HK Hong Kong	9	41
4.	AU Australia	6	1
5.	DE Germany	5	12
6 (tied)	GB United Kingdom	3	3
6 (tied)	IT Italy	3	3
7 (tied)	CN China	2	106
7 (tied)	RU Russian	2	20
8 (tied)	CA Canada	1	0
8 (tied)	ES Spain	1	1
8 (tied)	FR France	1	8
8 (tied)	IE Ireland	1	0
8 (tied)	KG Kyrgyzstan	1	0

Table 2. country/region distribution graph of malicious domains

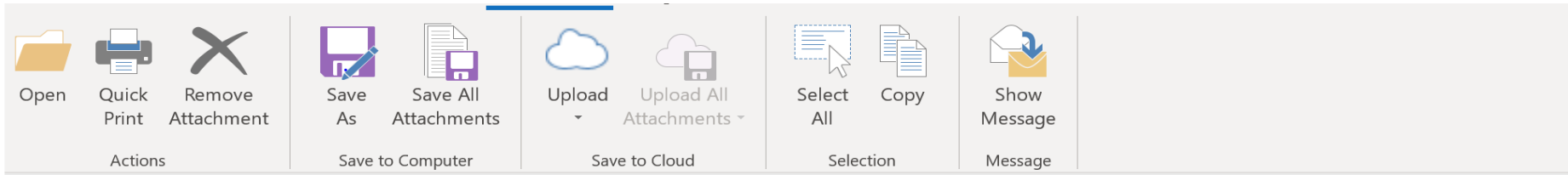
Web-based Threat Intelligence  
Addresses, Chirp



By Bo Qu, Tao Ye  
September 5, 2017  
Category: Unit 1  
7,576 likes

Malicious Web

# Phishing

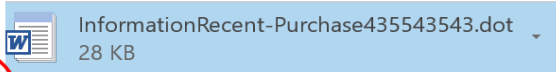


Wed 1/23/2019 10:11 AM

Apple <noreplymailmail5325476452@managements4.me>

Fw : [ Invoice Due (Copy) ] - Your recent purchase from App store "Partymasters - Fun Idle Game" - ( Wednesday, 23/01/2019. )

o cs@billingapple.com; cs@live.com



Dear Customer

Your account make a order on Apps Store,please visit your attachment

Billing Information

Sincerely,

Apple Support

[Apple ID Summary](#) | [Terms of Sale](#) | [Privacy Policy](#)

Copyright © 2018 Apple Distribution International

# Phishing

## Receipt 2019-0120



John LaMunyon <prjohn@SHLC.ORG>

Fri 2/1/2019 5:18 AM

You ▾



Dear Client,

We just processed the payment for your John LaMunyon account and charged your credit card for \$ 848.00. You will see "John LaMunyon" as recipient on your card statement.

Any question, please do contact us and we will be delighted to help.

Thank you for choosing John LaMunyon

Thank you in advance

### Invoice 2019-0120

**Sender:** John LaMunyon  
**Invoice date:** 01-30-2019  
**Due date:** 02-01-2019  
**Amount due:** \$0.00 (Amount paid: \$848.00)

[Get invoice](#)

# 2018 Reality

## Phishing

- **Openly Shared Public Data e.g. email addresses**
  - Address Book and other data can be used for “spoofing” and password spraying
  - Common passwords used in the local Seattle area
    - Fall2018
    - Winter2019
    - Seahawks12!
    - GoHawks!
    - Christmas2018
  - Vancouver area?
    - Canucks2019!
    - Lions2019!
    - Winter2019
    - Cannabis@@
    - Whistler2019

**Don't fall for this!**

# Ransomware

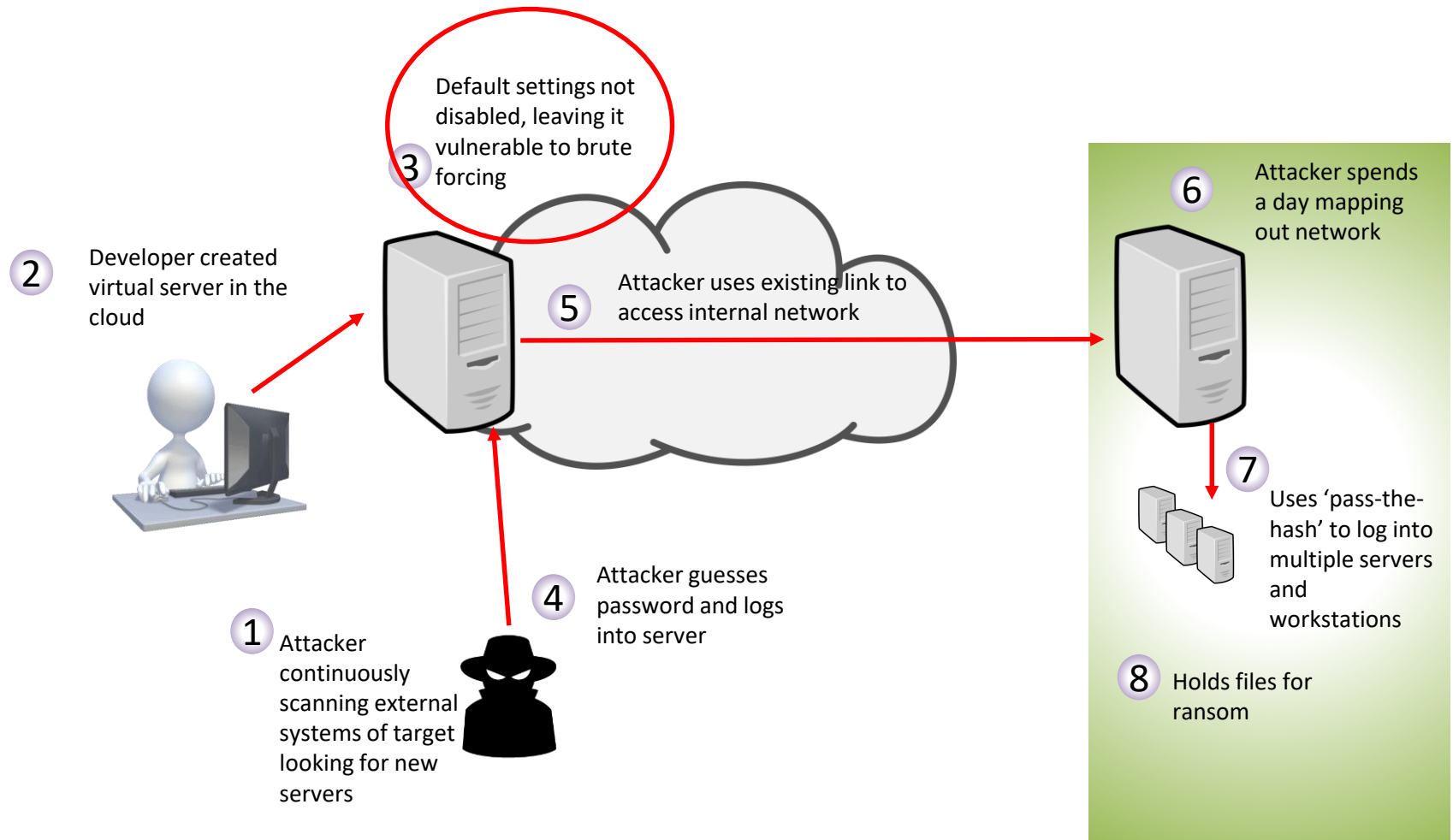
- WannaCry worm traveled between unpatched computers without user interaction.
- **March 14, 2017** - Microsoft issued critical security bulletin MS17-010
- **May 12, 2017** - WannaCry launched

*Lessons Learned:*

*“The answer is to patch systems earlier!”*



# 2018 Attack Chain Example



2018



# Attacks cities are seeing



- 400,000 cyberattacks blocked per month
- 70+% of incoming mail is SPAM or Phishing
- Outbound phishing from compromised internal accounts is a problem
- 10-15 successful phishing attacks per month

# 2018 Reality - A cyber-breach is inevitable

- Prepare for your breach:
- Test your recovery plan
- What you can do now to recover quickly?



# Looking ahead to 2019: Geopolitical Threats

- Hostile Nation States will use AI to manipulate your personalized news sources.
- Nation state will increase Disinformation Operations against trusted democratic institutions.
  - This is modern propaganda that is so tailored to the individual user that it becomes that persons reality.
  - Our political leaders are not trained to counter this threat and will struggle to discover truth from fiction.
    - Mob mentality, Brexit lies, American election candidate lies

# Looking ahead to 2019: Geopolitical Threats

- “Research has shown that 6 out of 10 of us will share an article just based on its title, which means in all of those cases, we're prone to fall for a hoax”
  - <https://www.cbc.ca/news/technology/fake-news-midterm-elections-1.4892305>
- Click bait sells ads. That is how the internet based information model works

# 2019 Geopolitical Threats: Your best defense

- Seek out the logical opposing view
  - When our news feeds show the opposing view as “idiots” be very cautious.
  - The opposition are logical people and they will present well thought out views. Always look for views that are presented as logical arguments.
- Most of life is not sensational.
  - Daily life is generally mundane. However it is the sensational that gets us to click on the link. Clicking on the link is what sells ads. That’s how the social media model works.

# 2019 Geopolitical Threats

- Nation-states have attacks on the shelf ready for cyberwar
  - [PressTV-Iran foils Israeli cyber attacks on communications ...](#)
    - [\*https://www.presstv.com/Detail/2018/11/05/579125/Iran-Israel-Cyber...\*](https://www.presstv.com/Detail/2018/11/05/579125/Iran-Israel-Cyber...)
    - 2018-11-05 · **Iran** says it has successfully staved off a wave of **cyber attacks** apparently by Israel targeting its communications infrastructure, vowing to pursue the ...
  - [Iran has laid groundwork for extensive cyberattacks on U.S ...](#)
    - [\*https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork...\*](https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork...)
    - July 20, 2018 - **Iran** has positioned **cyber** weapons to hit private firms and infrastructure, but there is no suggestion an **attack** is imminent, say U.S. officials.

# 2019 Predictions

## Threats Landscape: Looking ahead to 2019

- Cyber-attacks will become more methodical using AI
- Critical infrastructure ransomware attacks: OT, SCADA
- SPAM and phishing mails will rise to over 90% of total email received.
- Phishing will become very hard for a humans to detect.
- Cloud providers will continue to be slow for taking down malicious URLs.
- Legacy Applications risk increasing
  - Speed and ability to patch
- What else? Room discussion

Next year let's see what we missed. 😊



So where do we go  
from here?

# Information Security IndustryScape

## SECURITY MANAGEMENT AND COMPLIANCE

**Managed Security Service Providers**

IBM, at&t, verizon, Raytheon, hp, NTT, Dell, CSC, BT, Trustwave, Cisco, Symantec

**SIEM**

hp, EMC, RSA, McAfee, splunk, TIBCO, BlackStalax, EventTracker, LogRhythm, tenable, NetIQ, McAfee, Symantec, solarwinds

**Security Training**

SANS, wambol, HE ONE, SCIPP, AUSA, KnowBe4, Safelight, Fishnet Security, PHISHME, FishLine

**Governance, Risk and Compliance**

software, CMO, SAP, IBM, CYBERARK, protiviti, sas, enablon, mega, SAI GLOBAL, BWISE, RESOLVER, EMC, RSA, MetricStream, WYMAKO

## ENDPOINT SECURITY

**Secure Email Gateways**

SOPHOS, DELL, CLEAR SWIFT, mimecast, Barracuda, Trustwave, Fortinet, Websense, Proofpoint, Microsoft, Cisco, McAfee, Symantec, WatchGuard, Trend Micro, SilverSky

**Data Loss Prevention**

Absolute Software, Websense, Vormetric, McAfee, Symantec, Zecurion

**Endpoint Protection & Anti-virus**

IBM, Lumension Security, Webroot, Sophos, F-Secure, ARKON, Panda, Check Point, Threat Stack, Microsoft, Symantec, Kaspersky, Bitdefender, McAfee, ESET, LANDesk

**Endpoint Threat Detection & Response**

Avira, McAfee, ZoneFox, DTEX, PROMISE, TANIR, LogRhythm, ForeScout, Guidance, Nextthink

## IDENTITY AND ACCESS MANAGEMENT

**User Authentication**

HID, EMC, RSA, Entrust, Equifax, gemalto, mi-token, Vasco, TeleSign, Microsoft, Symantec, SecureAuth, Authentify, Duo, SafeNet

**Identity Governance and Administration**

Omada, anelogin, caradigm, SailPoint, eTrust, FISCHER, simeio, AlertEnterprise, Crossbas, Aveksa, okta, NetIQ, Centrify, bctsystems, EXOSTAR, Pingidentity

## INFRASTRUCTURE SECURITY

**Data Masking**

IBM, GreenSight, Informatica, Solix, Mentis, Axis, Voltage, Oracle

**Enterprise Network Firewalls**

Hillstone, Juniper, Cisco, AhnLab, Palo Alto, McAfee

**Intrusion Prevention Systems**

Stonesoft, McAfee, NSFOCUS, IBM, Enterasys, Cisco, HP, Radware, Sourcefire, Core Security

**Network Access Control**

ForeScout, Cisco, Juniper, Xixia, NADNetworks

**Unified Threat Management**

Hillstone, Sophos, Fortinet, Check Point, Rapid7, Barracuda, WatchGuard, Cisco

**Application Security**

Qualium, Veracode, Apprhority

**Application Firewalls**

Baracuda, Penta Security, Denial, Akamai, NSFOCUS, Radware, Citrix

**Application Control**

McAfee, Fortronics, Bit9, Veeva, Trend Micro, Arellia, Kaspersky

## SECURITY PARTNERS

UNISYS, fishnet, nexum, Atos, AccessIT, GuidePoint, ACCUVANT, THUNDERCAT, FUJITSU, cadre, BT, dimension data, FOREBYTE, NTT, GATHAM, DENIM GROUP

## SECURITY ORGANIZATIONS

**Education & Academic**

Security University, OWASP, Mississippi State, CSA, IANS, ISI, UTA, CIAC, UMUC

**Professional Associations & Certification**

(ISC)², GIAC, CompTIA, EC-Council, HISACA, FINANCIAL SERVICES, SANS, PCV, IANS, ISSA, TACIS, OWASP

**Government**

CESG, NIST, US-CERT, EUROPOL

## CYBER SECURITY

**Secure Web Gateways**

Blue Coat, Zscaler, Sophos, Intel, Trustwave, Symantec, Websense, Sangfor, Trend Micro, iboss

**Network Forensics**

IBM, IP, EMC, RSA, Blue Coat, WildPacket, NARUS, Riverbed, Netscout, Novetta, GigaVista

**Threat Intelligence Services**

EMC, RSA, NORSE, FOX IT, TEAM CYMRU, Symantec, ThreatStream, Check Point, VeriSign, SANS, IBM, VeriSign, WEERROOT

## CLOUD SECURITY

Blue Coat, Sophos, CloudPassage, Trustwave, Bitdefender, Zscaler, Wetsense, Symantec, Trend Micro, Cisco

## MOBILE SECURITY

**Mobile Data Protection**

Dell, Intel, CenterTools, Wave, Check Point, Symantec, Microsoft, Trend Micro, Kaspersky

**Mobile Device Management**

SAP, GLOBE, Citrix, Good, IBM, Soti, Absolute Software, Tangoe, Mobilitat, Sophos, LANDesk, ESE, Moxiana, Symantec

## SECURITY CONFERENCES

Gartner, Blackhat, RSA, InfoSecurity, SANS

## ANALYST HOUSES

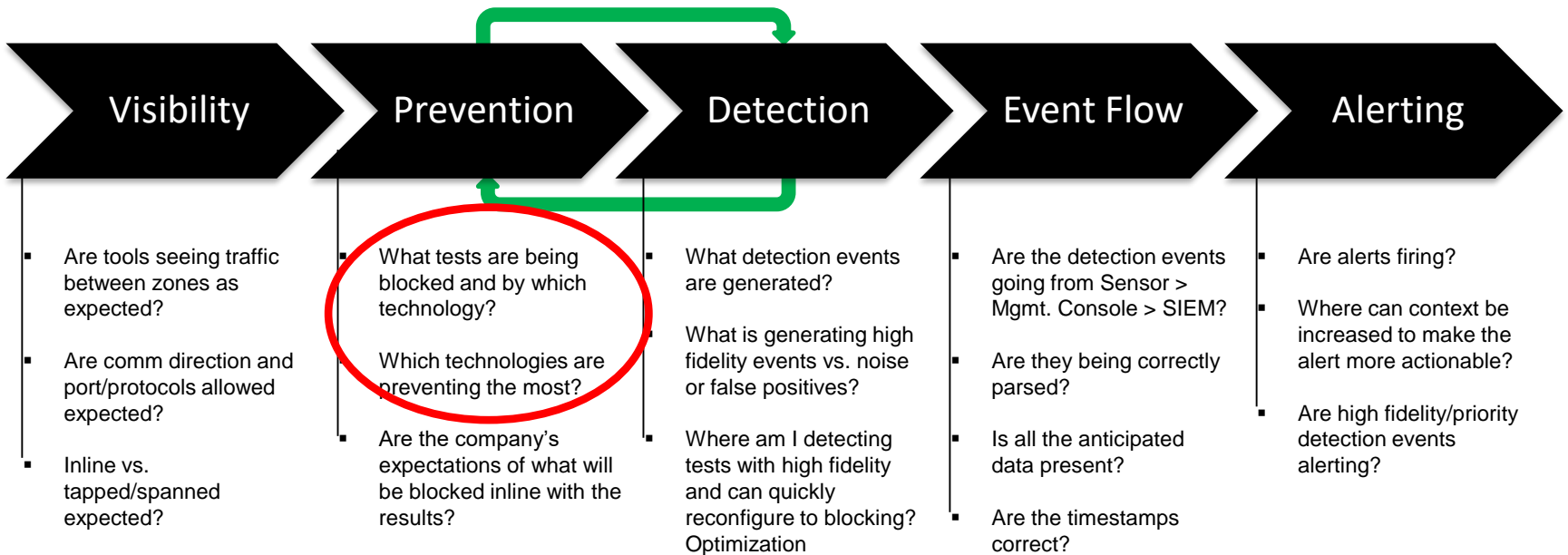
ASIS Research, Gartner, Quocirca, ESE, IDC, Forrester

Lots of Choices 😊

# Security Controls and security tool effectiveness

“So how will we know if all of this is working as the various vendors have promised?”

# EFFECTIVENESS VALIDATION PROCESS (EVP)



# POC At-a-Glance:

June 19-20, on-site at Seattle Municipal Tower

- 149 Actions ran
- 53% Block Rate
- 89% Events logged with Qradar
- Of those events, 11% triggered correlation alerts

**Controls tested: QRadar\*, FireEye\*, Websense, Checkpoint, Trend, Malware Bytes, InfoBlox**

Numbers may shift slightly once POC is complete

\*Indicates Verodin integrations for purpose of POC



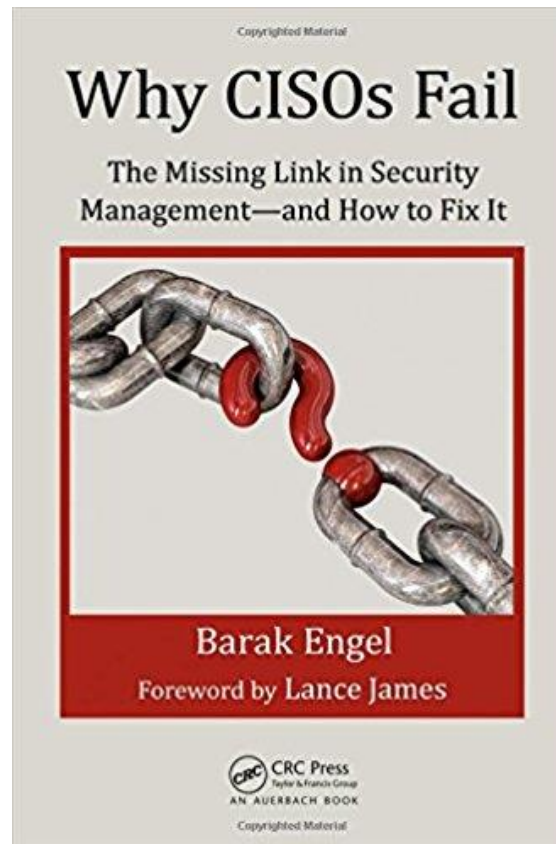
# Call to Action

- Learn from other industries as they might get hit before yours.
  - Attend information network opportunities such as Privacy & Security Conferences, BC Provincial Cybersecurity events, VanSecSig monthly broadcast meetings, AGORA and SecureWorld
- Know your IT Inventory and patch status
- Evaluate your threat models with the latest attack vectors. Ask, **“Can that happen here?”**
- Evaluate the effectiveness of your security controls
- Test your business continuity plans with a cyber attack scenario
- Cybersecurity risks needs to be part of the overall risk report delivered to your corporate Board of Directors.

# Call to Action: Specific Actions

1. Know your IT Inventory
2. Test and apply patches within the vendor & government guidelines. Critical patches ASAP
3. Implement SSL Inspection
4. Don't allow default passwords
5. Implement an anti-phishing solution that blocks outbound phishing from compromised internal accounts
6. Have threat hunting tools that are adaptive and use AI
7. Use a tool that verifies that your security tools are actually working.

# Good Reading



# Your Board of Directors

The screenshot shows the ISACA website interface. At the top, there is a navigation bar with links for Support, Shopping Cart, Join ISACA, Renew, Sign In, and ENGLISH. Below this is a search bar with 'ISACA' and 'My ISACA' tabs, a 'Site Content' dropdown, and a 'SEARCH' button. A main navigation menu includes ABOUT, MEMBERSHIP, CERTIFICATION, EDUCATION, COBIT, KNOWLEDGE & INSIGHTS, JOURNAL, and BOOKSTORE. A banner for 'CSX CYBERSECURITY NEXUS' is visible, along with a 'LEARN MORE >' link. The breadcrumb trail reads: ISACA > Knowledge & Insights > Research > Research-Deliverables > The Cyberresilient Enterprise: What the Board of Directors Needs to Ask. The main content area features the title 'The Cyberresilient Enterprise: What the Board of Directors Needs to Ask' in a large, dark font. To the right of the title is a 'Quick Links' section with a 'I want to...' dropdown and buttons for 'My Bookmarks' and 'Saved Searches'. Below the title, there are several action items: 'Download (registration required, 1M)', 'Also available in Chinese Simplified, Hebrew, Japanese and Spanish', 'Provide feedback on this document', and 'View News Release'. A thumbnail image of the document cover is shown. The main text begins with the heading 'Move Beyond Standalone Risk Protection to Enterprise Wide Risk Management and Operational Sustainability' and discusses the challenges of digital risk management in a modern marketplace.

ISACA > Knowledge & Insights > Research > Research-Deliverables > The Cyberresilient Enterprise: What the Board of Directors Needs to Ask

## The Cyberresilient Enterprise: What the Board of Directors Needs to Ask

Download (registration required, 1M)

Also available in Chinese Simplified, Hebrew, Japanese and Spanish

Provide feedback on this document

View News Release

### Move Beyond Standalone Risk Protection to Enterprise Wide Risk Management and Operational Sustainability

Advances in the digital marketplace are creating more opportunities for value—and risk. As organizations leverage cloud computing, the Internet of Things, mobile computing and social media, digital risk management takes on greater importance. Theft of personal information and private business information, misappropriation of resources, denial of service, and cybertheft are more common for enterprises large and small.

In the past, businesses used separate approaches to information security, business continuity and incident response. Today, a new comprehensive approach is required. The urgency of providing continuously available services for customers and business partners in a digital economy requires organizations to be resilient.

Learn how to make the important transition to becoming a cyberresilient enterprise with this thought-provoking resource that will help you:

#### Quick Links

I want to... My Bookmarks Saved Searches

- Explore certification opportunities
- Explore licensing and promotion opportunities
- Go to COBIT online
- View COBIT training opportunities
- Visit the Cybersecurity Nexus

PRIVACY &  
SECURITY  
CONFERENCE

My contact info:

[kevinmur@Hotmail.com](mailto:kevinmur@Hotmail.com)



# References:

- 
- baseStriker: Office 365 Security Fails to Secure 100 Million Email Users
  - <https://www.avanan.com/resources/basestriker-vulnerability-office-365>
- 
- How can Office 365 phishing threats be addressed?
  - <https://www.helpnetsecurity.com/2018/05/18/office-365-phishing-threats/>
- 
- Threat Spotlight: Cybercriminals Working Hard to Take Over Email Accounts
  - <https://blog.barracuda.com/2018/05/03/threat-spotlight-cybercriminals-working-hard-to-take-over-email-accounts/>
- 
- baseStriker attack technique allow to bypass Microsoft Office 365 anti-phishing filter
  - [http://www.cyberdefensemagazine.com/basestriker-attack-technique-allow-to-bypass-microsoft-office-365-anti-phishing-filter/?utm\\_source=hs\\_email](http://www.cyberdefensemagazine.com/basestriker-attack-technique-allow-to-bypass-microsoft-office-365-anti-phishing-filter/?utm_source=hs_email)
- 
- Fake Invoices: Why Does Office 365 Keep Missing These Phishing Attacks?
  - <https://www.avanan.com/resources/invoice-office-365-phishing>
- 
- ZeroFont Phishing: Manipulating Font Size to Get Past Office 365 Security
  - <https://www.avanan.com/resources/zerofont-phishing-attack>
-

# References:

- BC Office of information security
  - <http://www.gov.bc.ca/informationsecurity>
- VanSecSig
  - <http://www.infosecbc.org/events/>
- AGORA:  
[http://gallery.mailchimp.com/771fca6487cf0869f0a463e92/files/Agora\\_Acknowledgement.pdf](http://gallery.mailchimp.com/771fca6487cf0869f0a463e92/files/Agora_Acknowledgement.pdf)
- SecureWorld Expo Seattle Nov13-14, 2019
  - <https://www.secureworldexpo.com/>
- UBC Cybersecurity Summit:  
<http://konstantin.beznosov.net/professional/>
- UK National Cyber Security Centre: <https://www.ncsc.gov.uk/>

# What is your company doing?

- Thank You

# Defence Strategy

## Cybersecurity Operations Tool Suite:

- **Threat Hunting** – Threat intelligence from the security ecosystems community. Monitoring known bad URLs as they evolve
- **Endpoint Security** - (Next Gen A/V-EDR), Network Security (IDS/IPS/**SSL Inspection**), Email Security
- **Security focused SIEM and EDR** - integrated with A/D and strong user/machine based analytics (UEBA, XDR, ABA)
- **Anti-phishing** –Scans Outbound, Leverages AI, Integrates with FireEye Email Security
- **Log Correlation** - Events per Second Cost
- **Verification** -Test effectiveness of our controls

Defense in "Mesh"

The following slides are not intended as an endorsement for any particular product nor should in be considered a benchmark evaluation of the performance of any specific product. The performance results of your implementation will vary based on many factors within your company's IT ecosystem

# FireEye® Helix Ecosystem

## Helix Security Operations Platform



FireEye Network



FireEye Email



FireEye Endpoint

### Network Security & Cloud MVX:

- Automated Inline Blocking
- Multi-stage & Multi-Vector Detection
- Broad Coverage (Windows, OSX, many OS/file/app permutations)
- **SmartVision:** Protects from threats moving laterally within the network
  - Reduces the time to detection
  - Helps minimize risk of data theft
  - Helps reduce the spread of malware throughout the network

### Cloud Email Security:

- Correlation of stopped email-borne threats and attacks across environment
- Enhanced detection and alert fidelity
- Intelligence and rule books
- Alert prioritization
- Contextual intelligence
- Investigative tools

### Endpoint Security:

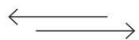
- EDR + EPP Capabilities; single agent
- Automated threat indicator sharing and context from Email & Network platforms
- Investigative tools and rapid remote containment for endpoints, even when outside of the enterprise
- Validate and analyze network traffic alerts
- Rapid interrogation of all endpoints



Users



FireEye Network Security



Firewall, IPS, SWG



Internet

The logo for RAPID7, featuring the word "RAPID" in white and "7" in orange, set against a dark grey rectangular background.

## insightIDR

- Detect stealthy behavior behind breaches.
- Key Features:
  - User Behavior Analytics (UBA)
  - Attacker Behavior Analytics (ABA)
  - Endpoint Detection and Visibility (EDR)
  - Centralized Log Management
  - Visual Investigation Timeline
  - Deception Technology



## Elastic Search

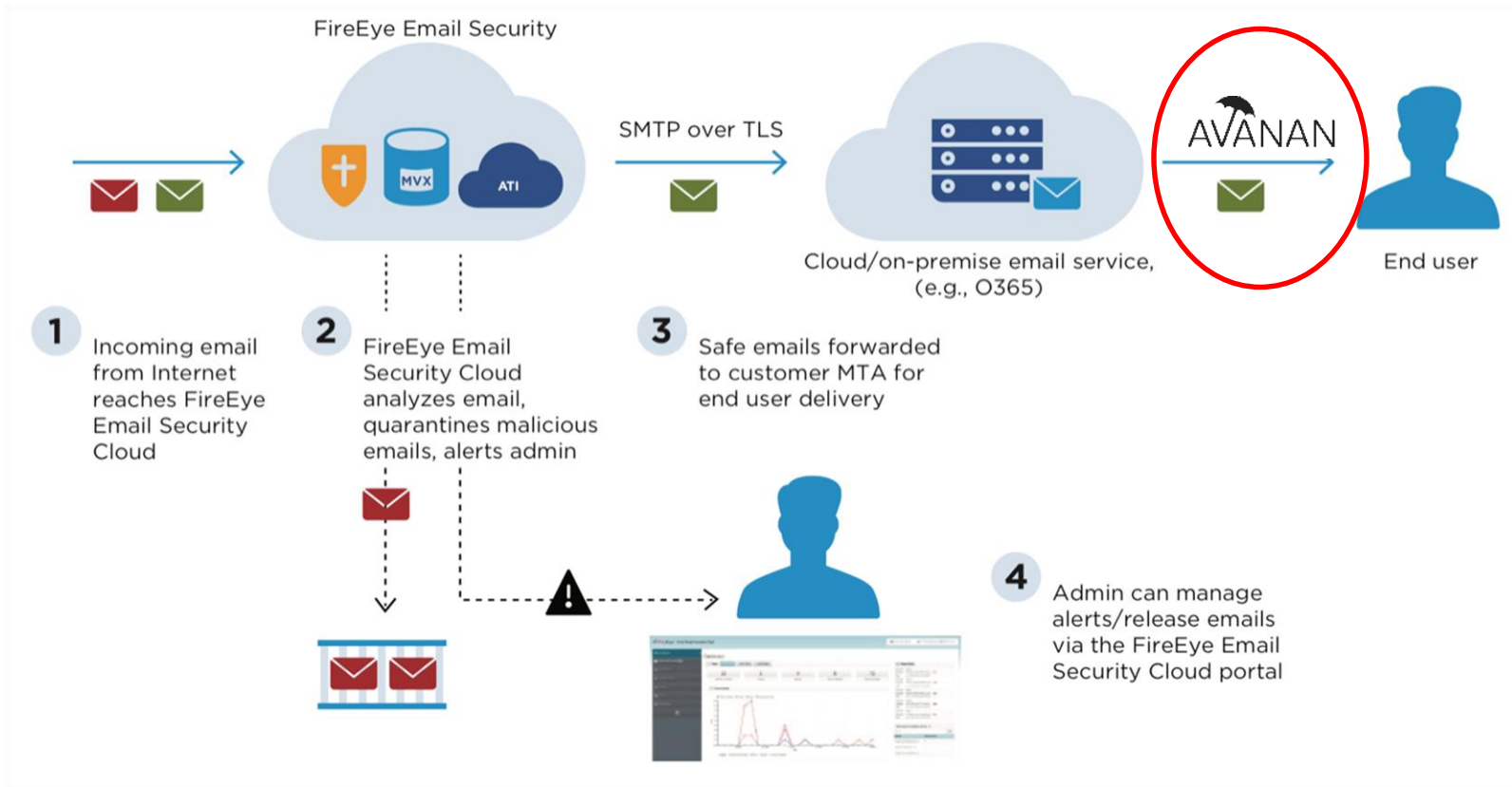
- Log collection/filtration to reduce Events per Second (EPS) cost
- Endpoint log collection
- Collection of O365 audit logs making them much more searchable
- Reduce the number of logging systems within the City. Reducing overall cost for the City.



## Avanan Anti-phishing solution

- Scans **outbound** email looking for phishing from compromised internal accounts
- Scans inbound mail like everyone else
- Incorporates with FireEye

# AVANAN



# 6 Cyber Attacks Business Networks will Face in 2018

## Malware

A malicious program installed on a PC. I.e. Trojans, worms, or adware.

**18%**

come from clicking malicious links in emails.

## Phishing

Uses social engineering to learn a user's password or personal data.

## Equifax

was a victim of this during a massive data breach in early 2017.

## Brute Force Password Attacks

A computer tries every possible combination for a password until successful.

## Denial of Service (DoS) Attacks

Overwhelms the network or servers with high volumes of traffic which disrupts all services.

## Man in the Middle (MITM) Attacks

The hardest to find. Pretends to be the destination for the information, copies it all, and then passes the information on to the real destination.

## Rogue software

Installs itself to do something that wasn't originally intended, often posing as something beneficial, like security software or a movie player.

**LOGICAL FRONT**

## Cyber Attacks by the Numbers

**43%**

of cyber attacks target small business\*

**64% of companies have experienced web-based attacks.**

**62% experienced phishing & social engineering attacks.**

**59% of companies experienced malicious code**

**51% experienced denial of service attacks.**