RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

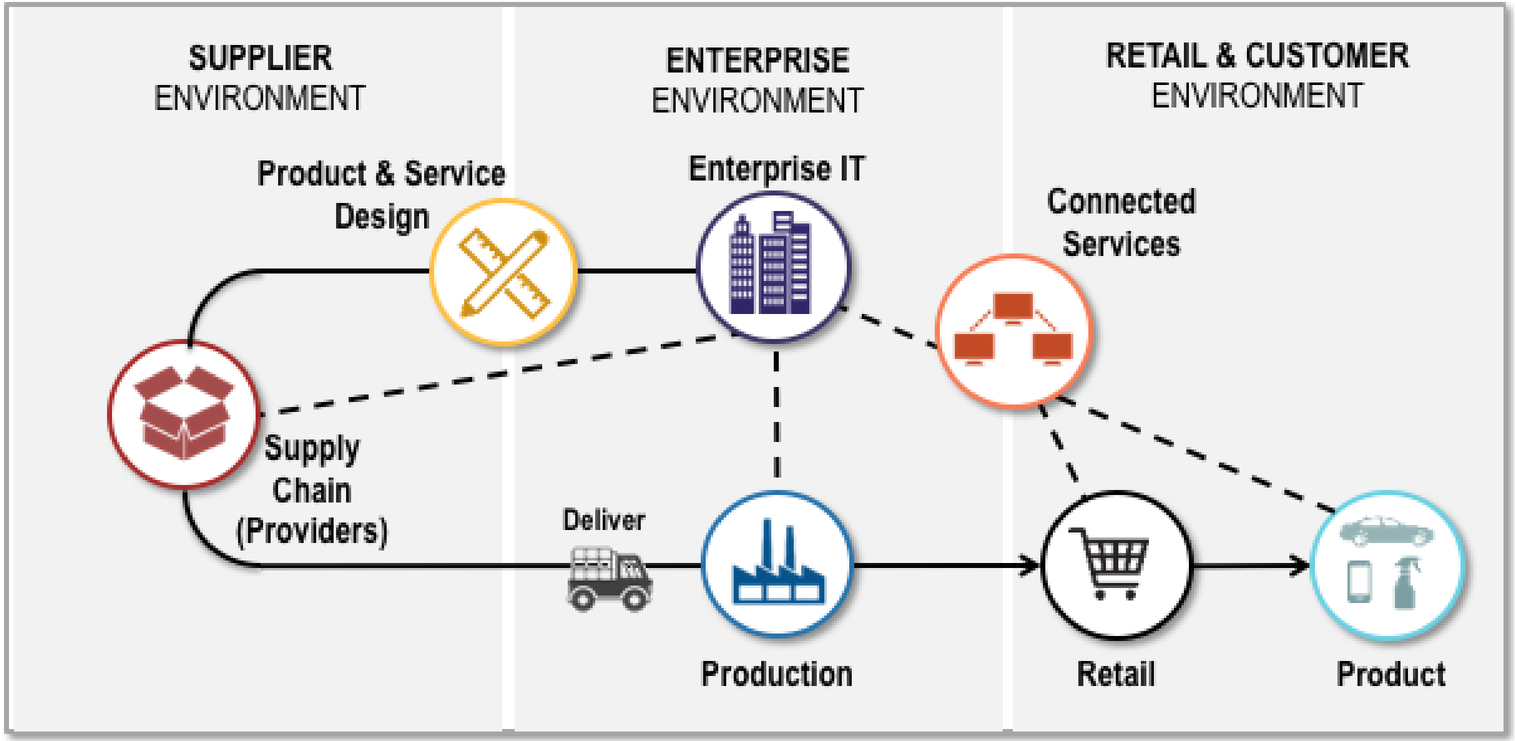
SESSION ID: TECH-T10

EVIDENCE-BASED SECURITY: THE NEW TOP FIVE CONTROLS

Todd Inskeep

Principal
Booz Allen Hamilton
@Todd_Inskeep

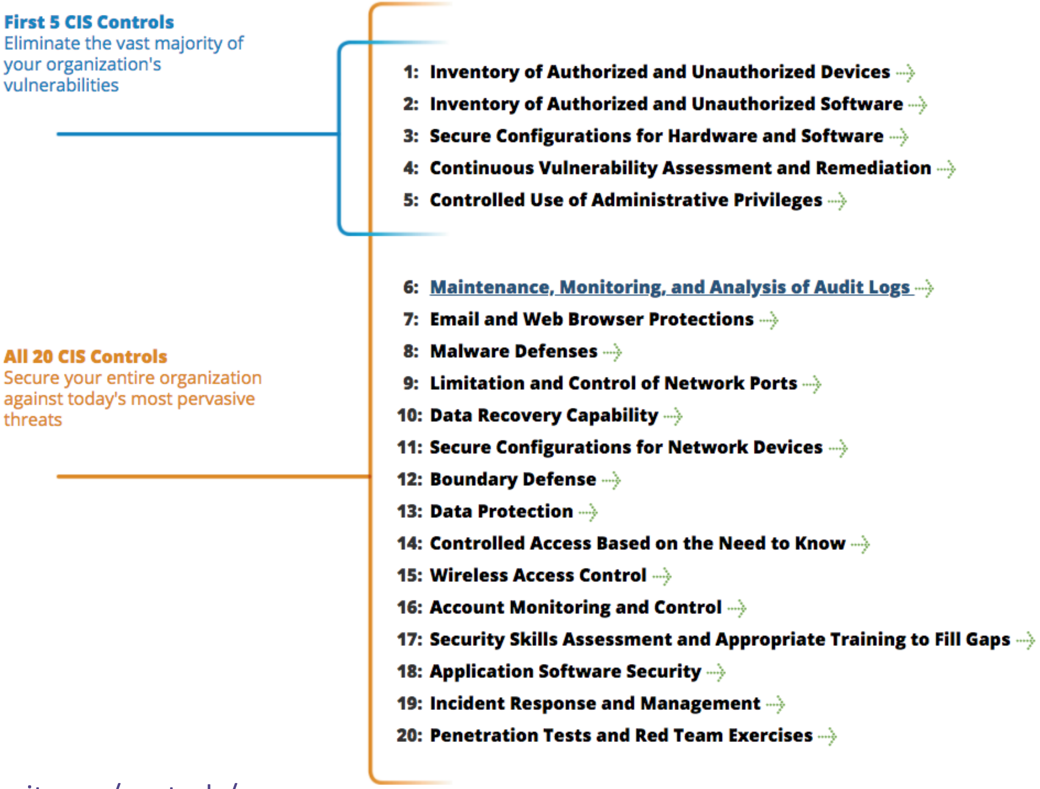
Where do you start protecting an enterprise?



Today’s CIS top 20 controls

- Published and maintains list of controls
- Often used as a starting point

➢ Because they reduce risk & some are *really hard to do*



First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

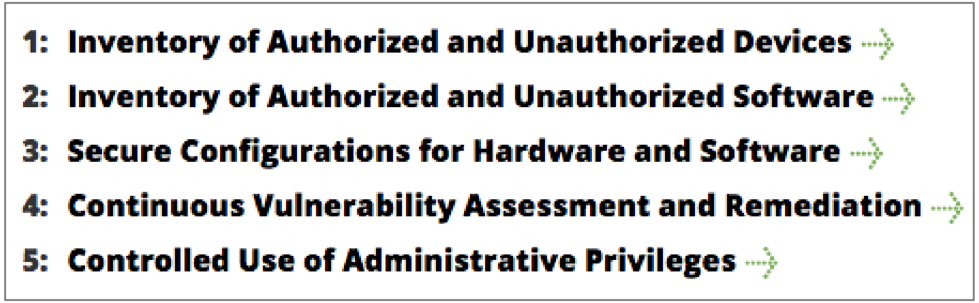
All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises

From: https://www.cisecurity.org/controls/

Are these top 5 really the best?

- In today’s threat environment, What should controls do?
  - Check the “we have security” box?
  - Meet compliance requirements?
  - Reduce Business Risk?
  - Or something else?



1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software

4: Continuous Vulnerability Assessment and Remediation

5: Controlled Use of Administrative Privileges

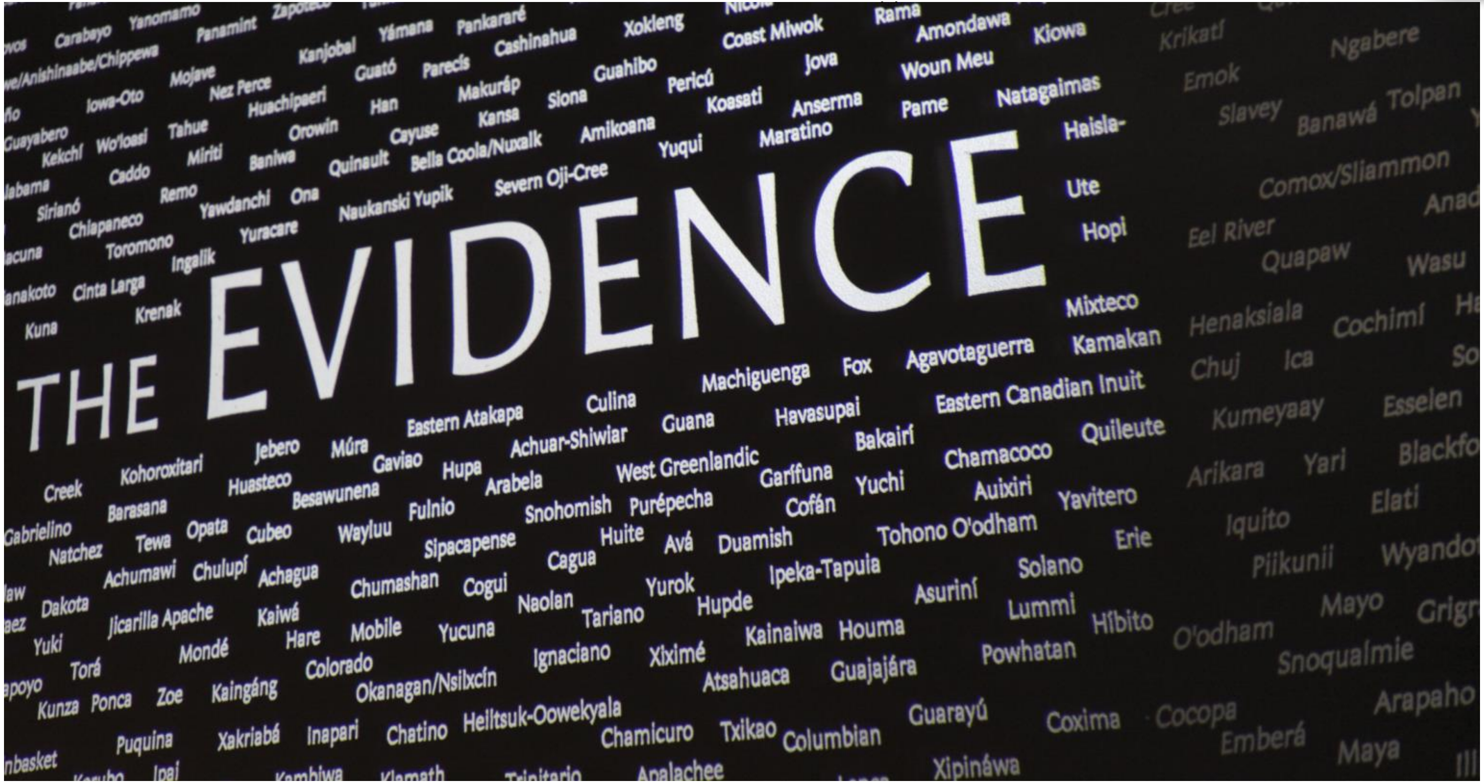


Image used with credit to
https://www.flickr.com/photos/generated/3408879691

Analyzed multiple data sources

- IT Governance List 742 incidents from Jan 2017-Mar 2018[1]
- Online Threat Alliance identified 159,700 total cyber incidents in 2017[2]
- “93% of breaches could have been prevented”[2]
- ➢ 2FA would have stopped or reduced the impact of every one

[1] Lewis Morgan – Monthly Notes at IT Governance https://www.itgovernance.co.uk/blog/author/lmorgan/

[2] Online Trust Alliance: https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

Considered the major attacks of 2017

Attack	Methodologies
SWIFT Attacks (2016)	Spearphishing, Credential misuse
HBO	Spearphishing, Credential misuse
Leaked Government Tools	Unknown – could be spearphishing, credential misuse, disgruntled insider
AWS Misconfigurations	Scan for vulnerabilities, Credential misuse
WannaCry	Privilege escalation, credential misuse
NotPetya	S/W Supply chain exploit, Privilege escalation, credential misuse
Equifax	Scan for vulnerabilities, Credential misuse
Ransomware	Spear/phishing
Bad Rabbit	Spear/phishing, privilege escalation, credential misuse,

Examined our experience

Financial Services

- 17 of the Top 25 US FIs

Banking

Exchanges

Hedge Funds

Insurance

Transportation

- Multiple automakers/ OEMs

- Multiple US-based Airlines

Automotive

Technology

Aviation

Logistics

Health & Life Sciences

- 4 of the Top 15 Bio-Pharma's + Ultra-rare

Biotech

Medical Devices

Pharmaceutical

Energy

- Fortune 50 Super-Major Oil & Gas companies

Utilities

Oil & Gas

Nuclear

How do breaches and attacks start?

- ❑ Evidence: Phishing & Spearphishing
  - Spear phishing is the number one infection vector employed by 71 percent of organized groups in 2017 (Symantec ISTR)
  - Phishing & Spearphishing are significant attack vectors across attack groups and methods (Crowdstrike GTR)
  - 66% of malware from email attachments (Verizon DBIR)
- ❑ Solution: **Technical Email Controls**
  - Active Spam & Phishing controls
  - Sandboxing, prefetch
  - DMARC, SPF, DKIM
  - Track 'Clicks'
  - Mark 'external' email

Wait, how do breaches start?

- Evidence: Clicking on Links or Opening Attachments
  - 90% of incidents due to human error (OTA)
  - More than 1/3 of inadvertent activity involved attackers tricking users with links and attachments (IBM X-Force)
  - Click rates of 7-14% are typical and vary by industry; much higher rates are surprisingly common (Verizon DBIR)
- Solution: **Train Users To Spot Spear/Phishing**
  - Mark ‘external’ email
  - Enable easy user reporting
  - Phish yourself
  - Manage incentives and penalties

How do attackers get in and move laterally?

- Evidence: Privileged access - stolen or weak passwords
  - 81% of incidents involved weak or stolen passwords or both;
    “only a single-digit percentage of breaches…involved exploiting a vulnerability” (Verizon DBIR)
  - Stolen credentials were the most commonly seen lateral movement technique (Symantec)
  - More than 1/3 of inadvertent activity involved attackers tricking users with links and attachments (IBM X-Force)
  - Multi-factor authentication would have stopped or reduced the impact of virtually every attack in 2017 (& 2016, 2015, 2014….)
- Solution: **Implement multifactor authentication & manage privileged access**
  - Virtually any kind of two-factor solution is better than none
  - Especially for privileged users and administrators
  - Manage privileges, privilege groups, stored & cached credentials, and privilege groups

How do attackers “break systems’

- ❑ Evidence: Exploiting known vulnerabilities
  - Time to Patch a known vulnerability is 6 weeks or more (Verizon DBIR)
  - Misconfigured servers and networked backup incidents exposed more than 2 billion records in 2017 (IBM X-Force)
  - **Zero day attacks used by only 27 percent of the 140 targeted attack groups tracked by Symantec**
  - Privilege escalation through known vulnerabilities is commonly used by attackers (Crowdstrike)
- ❑ Solution: **Patch Quickly & Configure Properly**
  - Scans for vulnerabilities and configuration issues regularly
  - Patch & fix identified vulnerabilities promptly
  - Especially on Internet facing systems

Where do attackers start?

- Evidence: Exploiting known vulnerabilities
  - Overall targeted attack activity is up by 10 percent in 2017 (Symantec)
  - Trade secrets, followed by personal information are the top data targets (Verizon DBIR)
  - Top targeted industries are: financial services, info & comms technology, manufacturing, retail, and professional services (IBM X-Force)
  - eCrime groups and nation states target specific victims (Crowdstrike)
  - Every adversary threat model starts with reconnaissance
- Solution: **Verify what's facing the world** & lock it down
  - Use red teams to simulate adversary activity attacks
  - Learn from offer external scans and risk scores
  - Assess business and technology connections (aka dependencies)
  - Especially on Internet facing systems
  - Limit Internet Points of Presence; establish strong gateways/DMZs

The new Top Five

1. Implement multifactor authentication (MFA) & privileged access management
2. Email technical controls
3. Train users to spot Spearphishing
4. Manage vulnerabilities well
5. Verify what’s facing the world & lock it down

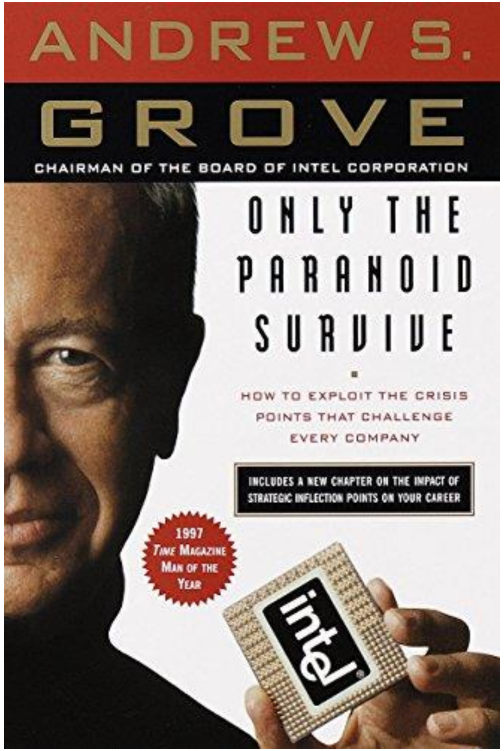
Are there really only two kinds of companies?

Largest Health Insurance Providers	# of Subscribers	#of Data Records Lost to Cyber Incidents (2012-2017)
1. United Healthcare	70 million	0
2. Anthem	39.4 million members	78 million[1]
3. Aetna	23 million members	12,000
4. Health Care Services Corp.	15 million members	0
5. Cigna	14.7 million members	0
6. Humana,	14.23 million members	3,831
7. Centene Corp.	11 million members	0
8. Kaiser Permanente	10.7 million members	8020
9. Highmark	5.3 million members	0
10. WellCare Health Plans	3.68 million members	24,809
Totals:	~207 million members	~78 million

[1] The # of records lost at many companies exceeds the number of subscribers because the records of multiple family members may be associated with a single subscriber; in some cases, both current and past customer information was lost.

Note: Companies that did not report a cybersecurity incident may have reported loss due to physical theft, employee negligence, or other factors.

How do these and other companies succeed?

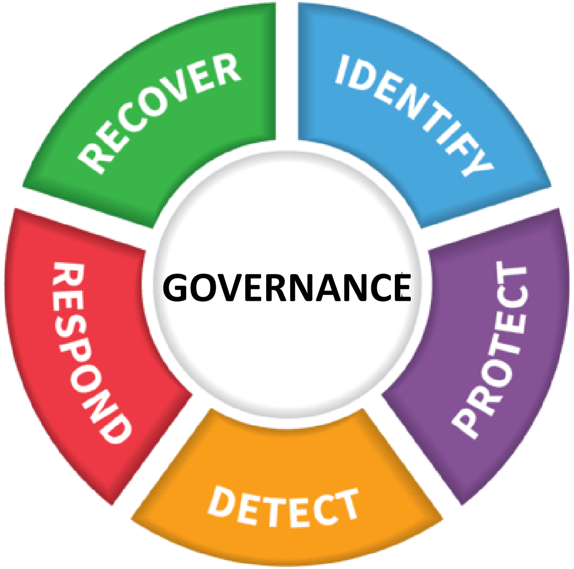

ANDREW S.
GROVE
CHAIRMAN OF THE BOARD OF INTEL CORPORATION
ONLY THE PARANOID SURVIVE
HOW TO EXPLOIT THE CRISIS POINTS THAT CHALLENGE EVERY COMPANY
INCLUDES A NEW CHAPTER ON THE IMPACT OF STRATEGIC INFLECTION POINTS ON YOUR CAREER
1997 TIME MAGAZINE MAN OF THE YEAR
intel

- Nation-states and Criminals are looking for their information
- Breach notification laws require reporting
- Under Executive Order 13636, the government notifies companies when they are the target of an incident.

➤ Focus on preparation based on reality

Some bonus ideas

- Practice and plan for major incidents
- Establish network & endpoint visibility for early detection
  - Breakout time <2 hours
  - Dwell time ~86 days
- Review software supply chains & update processes
- Exercise realistic cyber incident plans
- Find comprehensive threat intelligence services and automate integration
- Support a culture of innovation around all aspects of the NIST Cybersecurity Framework



https://www.nist.gov/cyberframework

When you get back to the office

- Review privileged account usage throughout the organization and investigate/implement MFA
  - Begin Planning the implementation of MFA – even periodically for some applications that address APIs with privilege
- Lock down email, DMARC/SPF/DKIM, Sandboxing, URL blocking attachment screening, marking email “External”
  - Think about anything that gives your users an edge –
- Expand phishing training – hit everyone with it on an irregular, but frequent basis increase awareness
  - Then phish yourselves – use outlook/email tool buttons to increase reporting
- Update vulnerability management processes planning
  - Focus on using inventory and architecture to drive patching the right things
- Review pentesting and red teaming plans – use external tools to look at yourselves from outside – like the bad guys do
  - Lock down anything that’s externally facing – especially cloud services from AWS & Axure to Google Docs, Salesforce and ServiceNow.

APPENDIX

References – partial list

- IT Governance – list of 742 incidents from Jan 17- Mar 18 (Lewis Morgan – Monthly Notes at IT Governance https://www.itgovernance.co.uk/blog/author/lmorgan/)
- Online Trust Alliance - Cyber Incident Trends Report: https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
- Verizon Data Breach Investigation Report (Apr 2017) (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/)
- IBM X-Force Threat Intelligence Index March 2018 (https://www.ibm.com/security/data-breach/threat-intelligence)
- Crowdstrike Global Threat Report (Feb 26, 2018) (https://go.crowdstrike.com/CrowdStrike-Threat-Report.html)
- Symantec 2018 Internet Security Threat Report (March 22, 2018) (https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf)
- Harvard Business Review - https://hbr.org/2017/12/which-of-your-employees-are-most-likely-to-expose-your-company-to-a-cyberattack (Dec, 2017)
- 2017 Healthcare Breaches - 2017 Breach Report: 477 Breaches, 5.6M Patient Records Affected https://www.healthcare-informatics.com/news-item/cybersecurity/2017-breach-report-477-breaches-56m-patient-records-affected
- Aetna fined for 12,000 lost records - https://healthitsecurity.com/news/17m-settlement-agreement-reached-in-aetna-data-breach-case
- 10 Largest Health care organizations by membership - http://www.beckersasc.com/asc-coding-billing-and-collections/the-10-largest-health-insurance-companies-by-membership.html
- RSA Phishlabs reporting: https://info.phishlabs.com/blog/rsa-2018-preview-phishing-trends-intelligence-report

Highlights - Symantec

- Symantec 2018 Internet Security Threat Report (March 22, 2018) (https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf)
  - targeted attack activity is up by 10 percent in 2017, motivated primarily (90 percent) by intelligence gathering.
  - Spear phishing is the number one infection vector employed by 71 percent of organized groups in 2017. The use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups tracked by Symantec
  - 1 in 13 Web requests lead to malware Up 3% from 2016
  - ~140 groups of attackers, criminal, nation-state and intelligence gathering
  - stolen credentials were the most commonly seen lateral movement technique employed. Attackers often use hacking software tools to obtain credentials from a compromised computer and then use them to attempt to log into other computers on the network.
  - There was at least one large software update supply chain attack reported every month in 2017.

Highlights - Crowdstrike

- Crowdstrike Global Threat Report (Feb 26, 2018) (https://go.crowdstrike.com/CrowdStrike-Threat-Report.html)
  - Trickle-down of military grade cyberweapons to mass criminal use & concommitent use of criminal attacks like ransomware in nation-state attacks
  - Breakout time of <2 hours to move laterally
  - Average Dwell time – 86 days
  - Slow Down Attackers
    - limiting user account permissions
    - application whitelisting
    - segregating users and networks,
    - And aggressively applying available patches.

Highlights – IBM X-Force

- IBM X-Force Threat Intelligence Index March 2018 (https://www.ibm.com/security/data-breach/threat-intelligence)
  - Ransomware attacks cost more than $8B (US) globally in 2017
  - Misconfigured cloud servers and networked backup incidents unintentionally exposed more than 2 billion records
  - More than one-third of inadvertent activity experienced by X-Force-monitored clients involved attackers attempting to trick users into clicking on a link or opening an attachment.

Highlights - Verizon

- Verizon Data Breach Investigation Report (Apr 2017) (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/)
  - 81% of breaches used stolen/weak passwords
  - 66% of malware from email attachments
  - Breach timelines continue to paint a rather dismal picture—with time-to-compromise being only seconds, time-to-exfiltration taking days, and times to discovery and containment staying firmly in the months camp. Not surprisingly, fraud detection was the most prominent discovery method, accounting for 85% of all breaches...
  - Phishing was again the top variety, found in over 90% of both incidents and breaches.

Highlights - RSA

- RSA Phishlabs Early Report (https://info.phishlabs.com/blog/rsa-2018-preview-phishing-trends-intelligence-report)
  - Targeting shifted to Enterprise users
  - Webmail now #1 target vs FS before
  - Number of Office 365 Attacks
  - Shift to enterprises
  - Phishing on SMS & Social Media growing