RSA®Conference2019
Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: SDS-W01

Maximising Your Return on Security Investments

Wayne Tufek

Director
CyberRisk

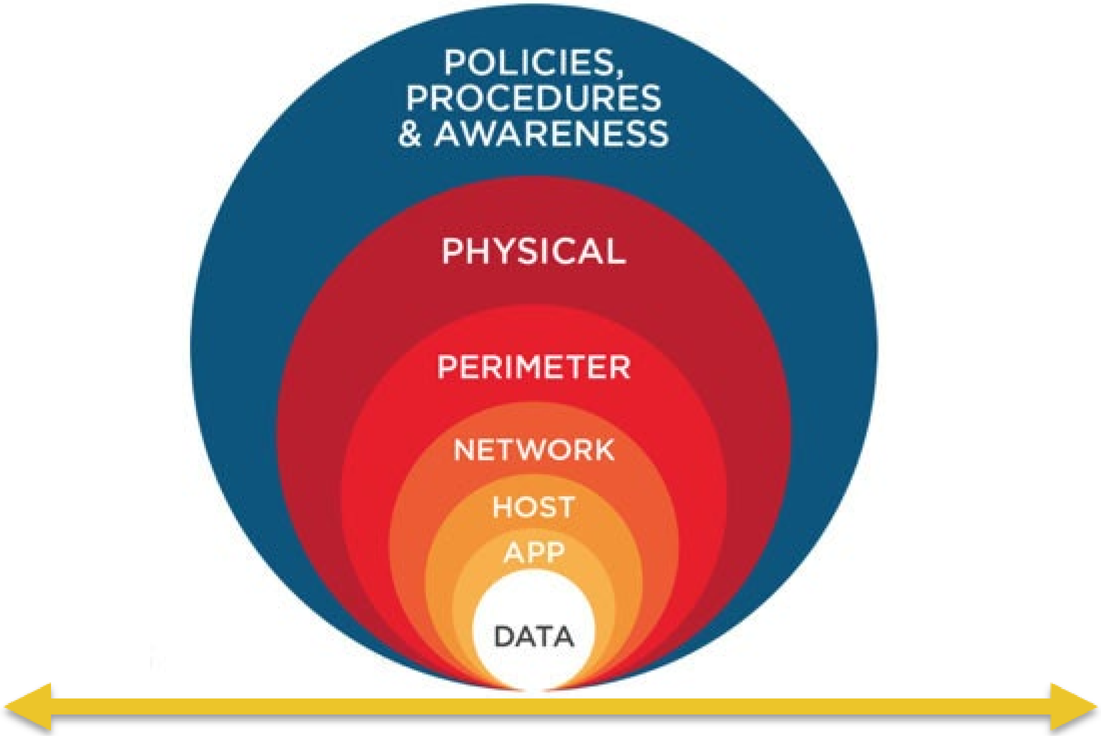
Agenda

- Introduction
- Objectives
- Horizontal defence in depth
- Vertical defence in depth
- Minimum viable security
- Tools
- Putting it all Together
- Questions

Objectives

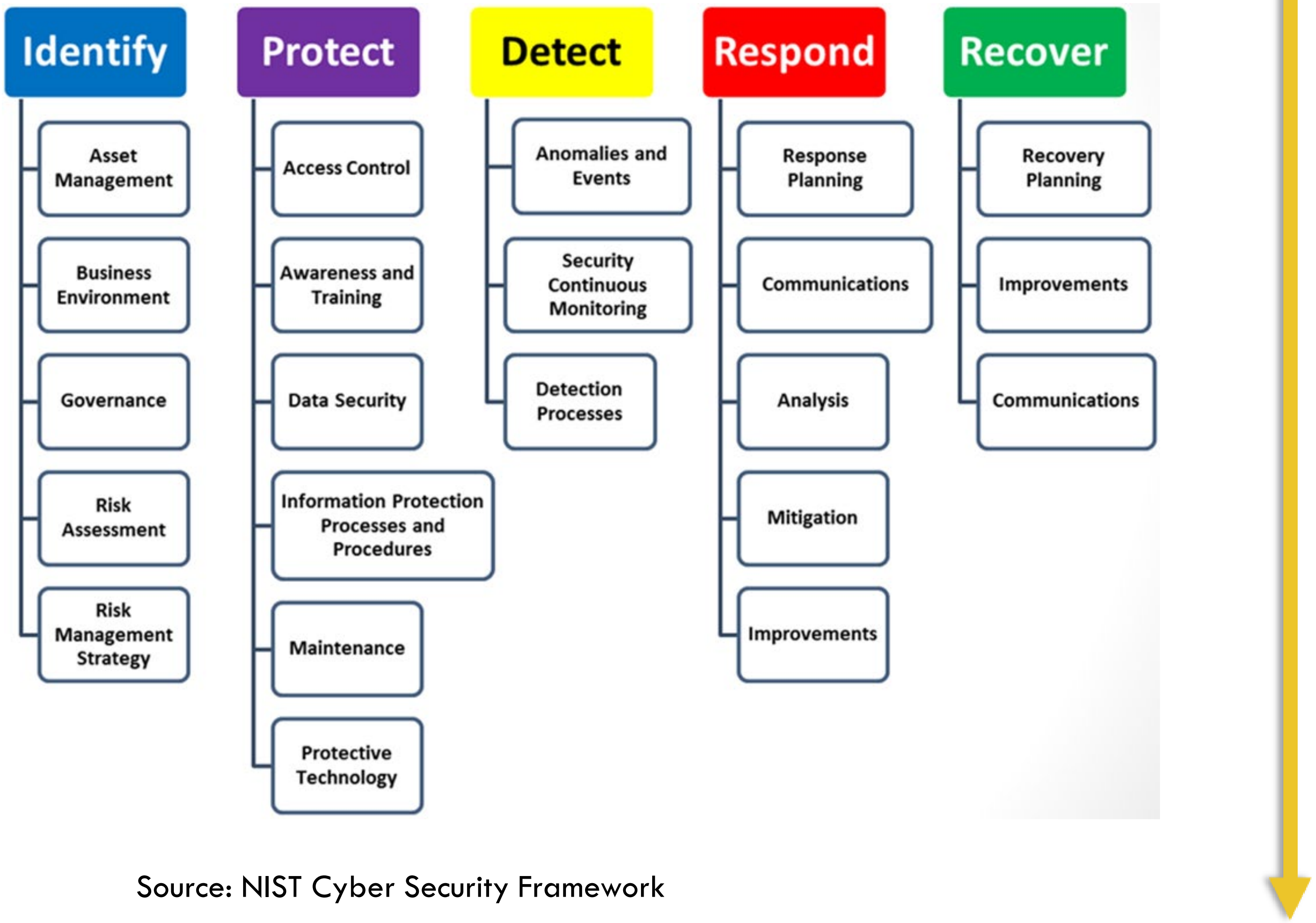
1. Understand the tools and techniques available to design a pragmatic and practical security architecture
2. Understand the key controls that make up basic cyber security hygiene
3. Understand the security investment portfolio approach to cyber security

Horizontal defence in depth



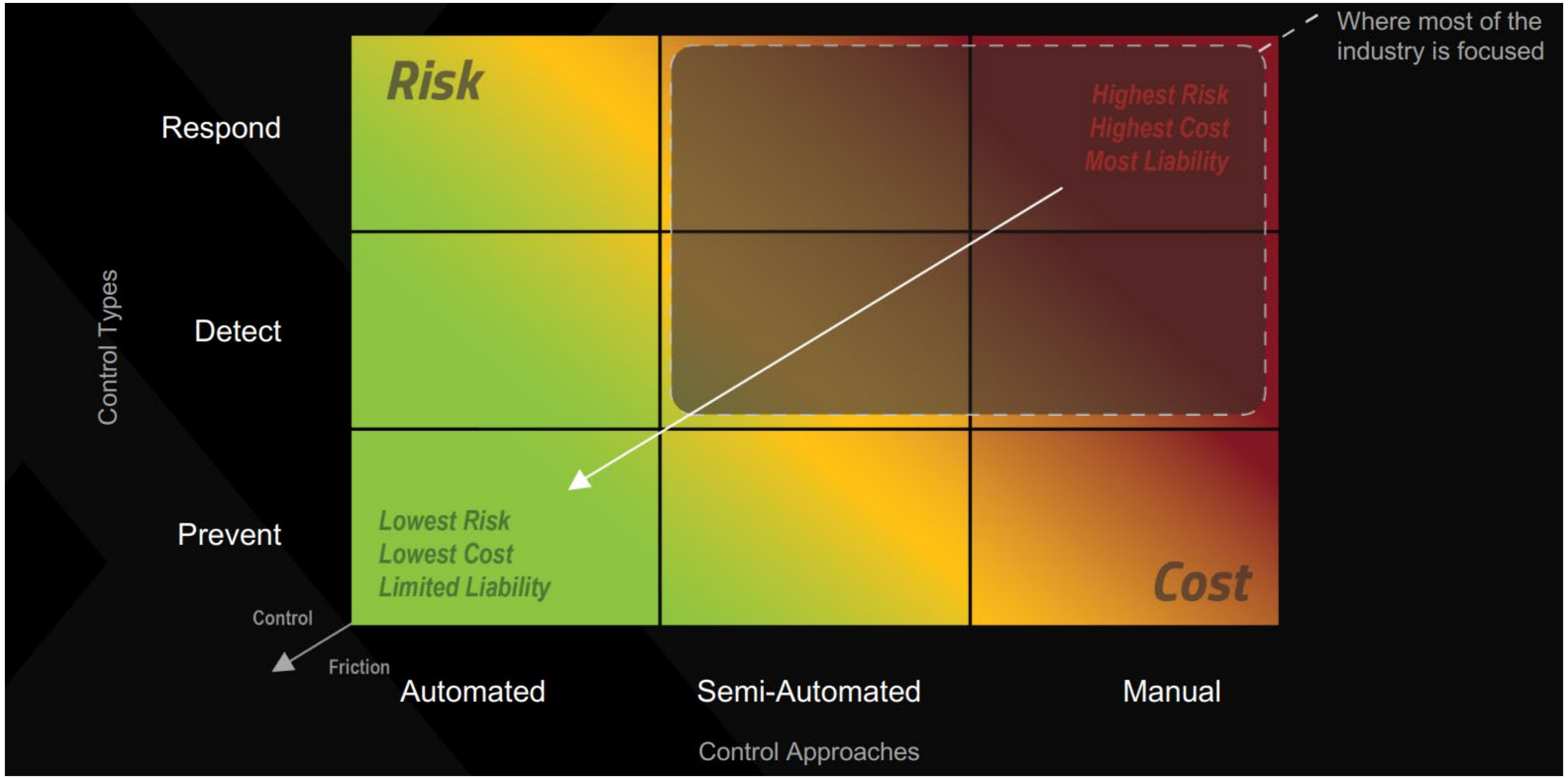
Source: http://www.matrixcc.net/cyber-defense/

Vertical defence in depth



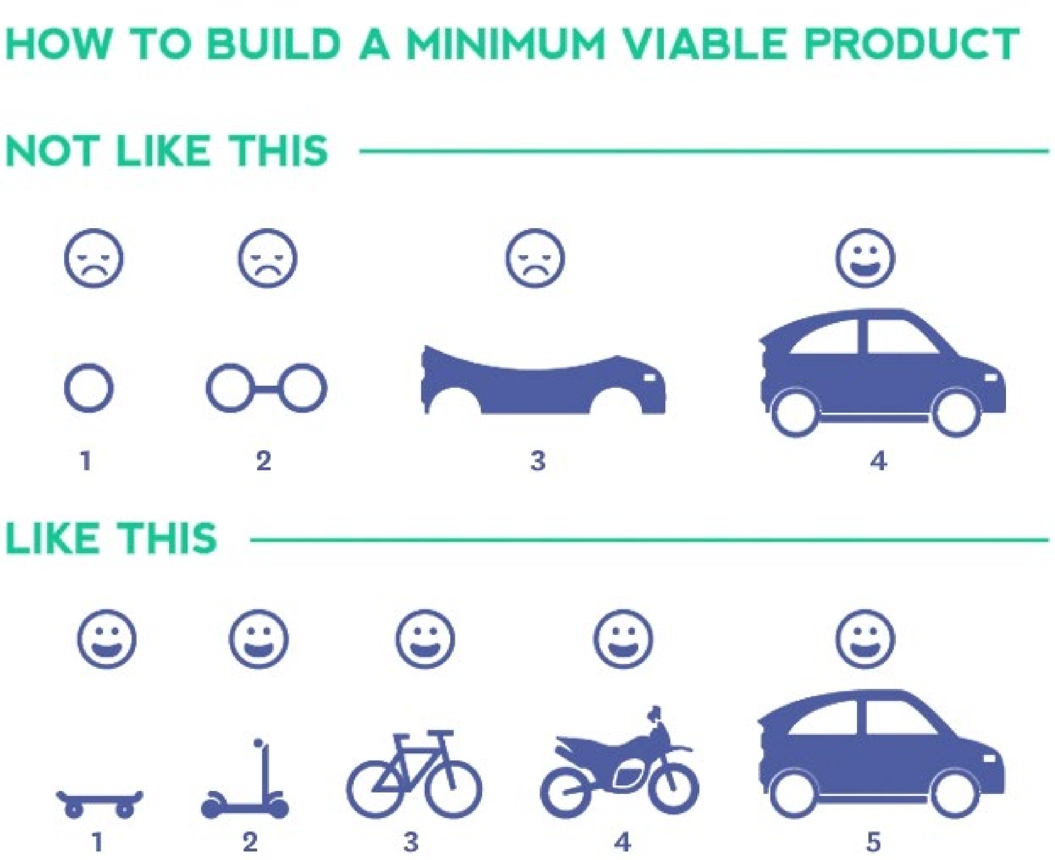
Source: NIST Cyber Security Framework

Vertical defence in depth



Source: Cylance
https://www.slideshare.net/PECBCERTIFICATION/trust-and-the-economics-in-the-age-of-information-security

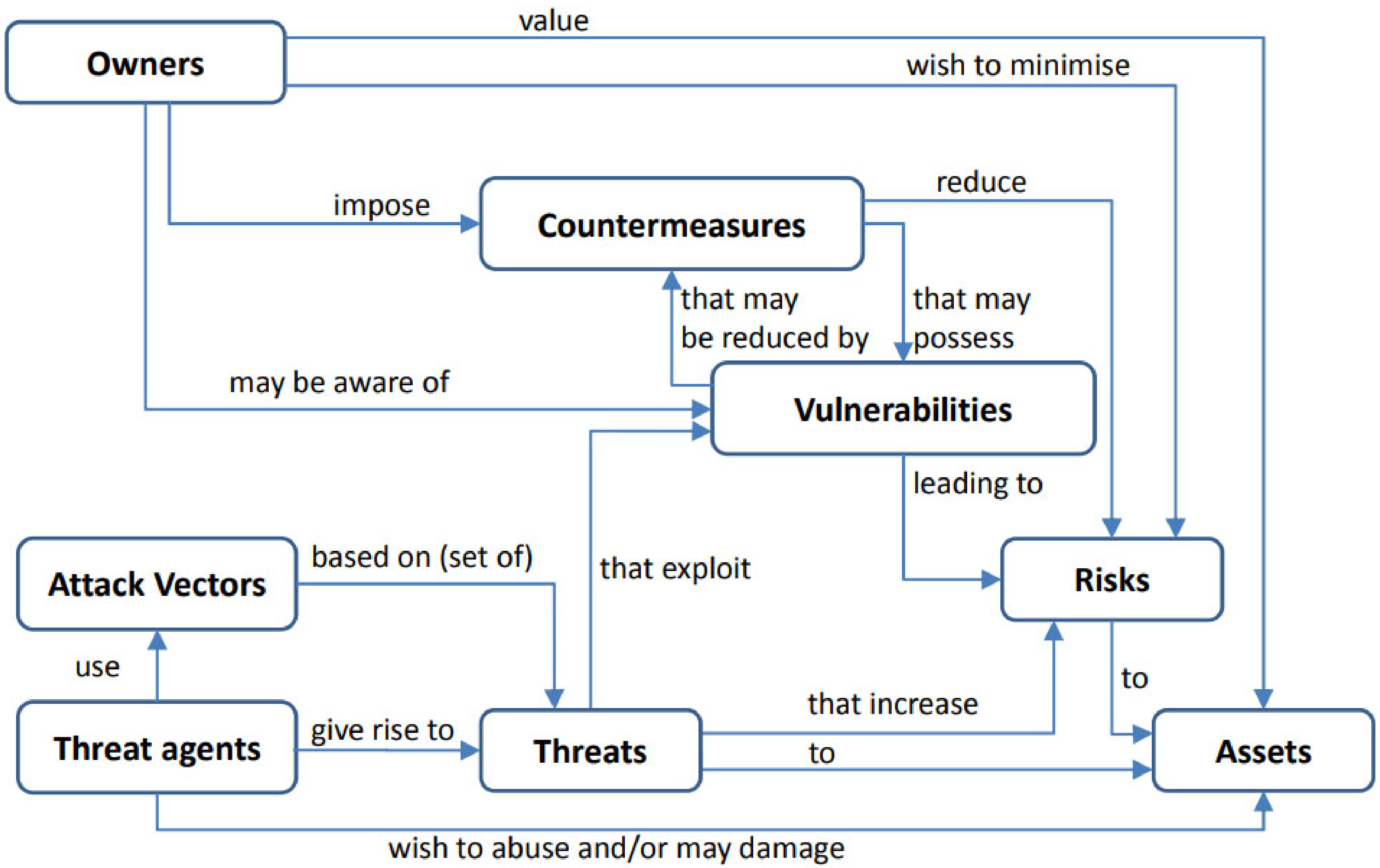
Minimum viable security



Source: https://blog.kartones.net/post/mvp-minimum-viable-product/

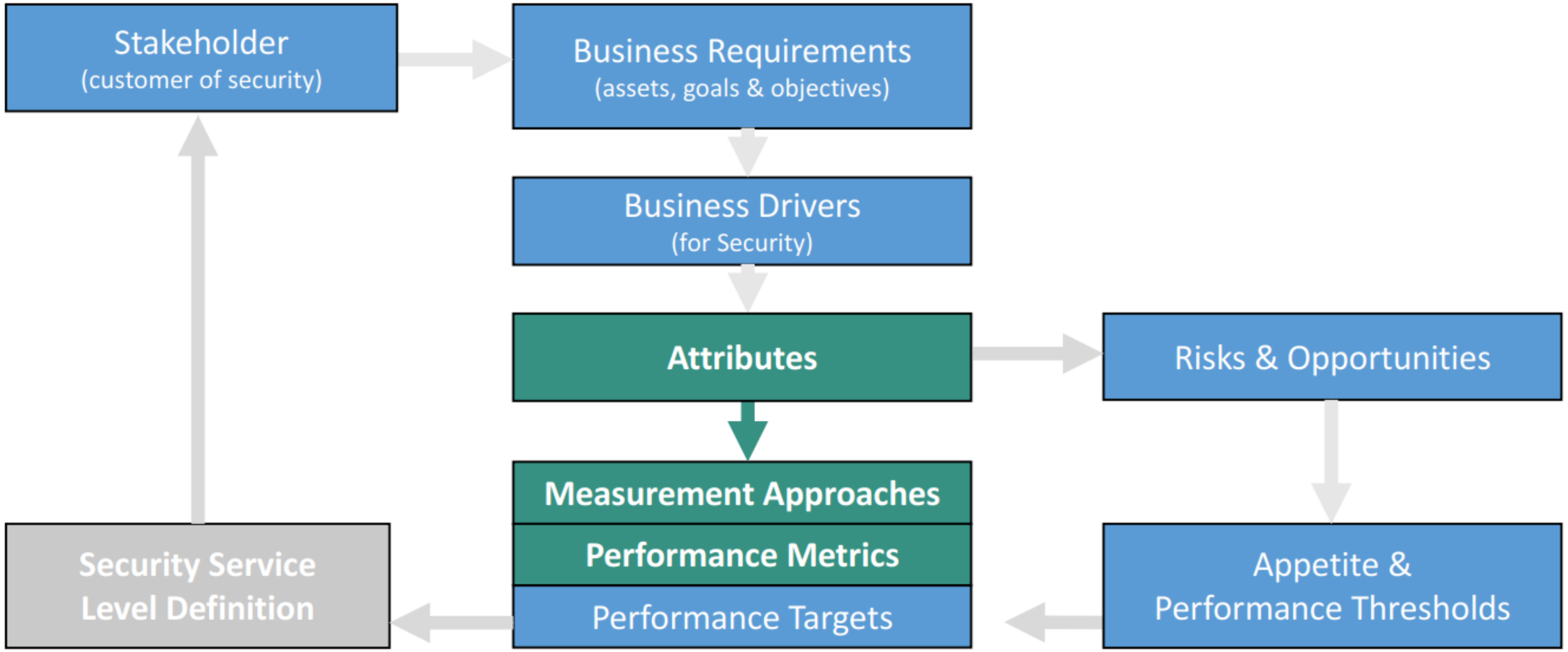
Information security in a diagram

Asset (*Vulnerabilities, Controls*), **Threat** (*Threat Agent Profile, Likelihood*) and **Impact**.



Source: http://sagenetcom.com/security/

Sherwood applied business security architecture



Source: David Lynas Consulting
https://sacramento.iiba.org/sites/sacramento/files/Events/201709/Introduction%20to%20SABSA%20for%20BAs%20-%20Sac%20Valley%20IIBA%2009.20.17%20FINAL.pdf

Sherwood applied business security architecture

- *So, what is an Attribute?*
- SABSA define an attribute as a conceptual abstraction of a real business requirement (the goals, objectives, drivers and targets) which are modelled into a normalised language that articulates requirements and measures performance in a way that is instinctive to all stakeholders.

Source: SABSA

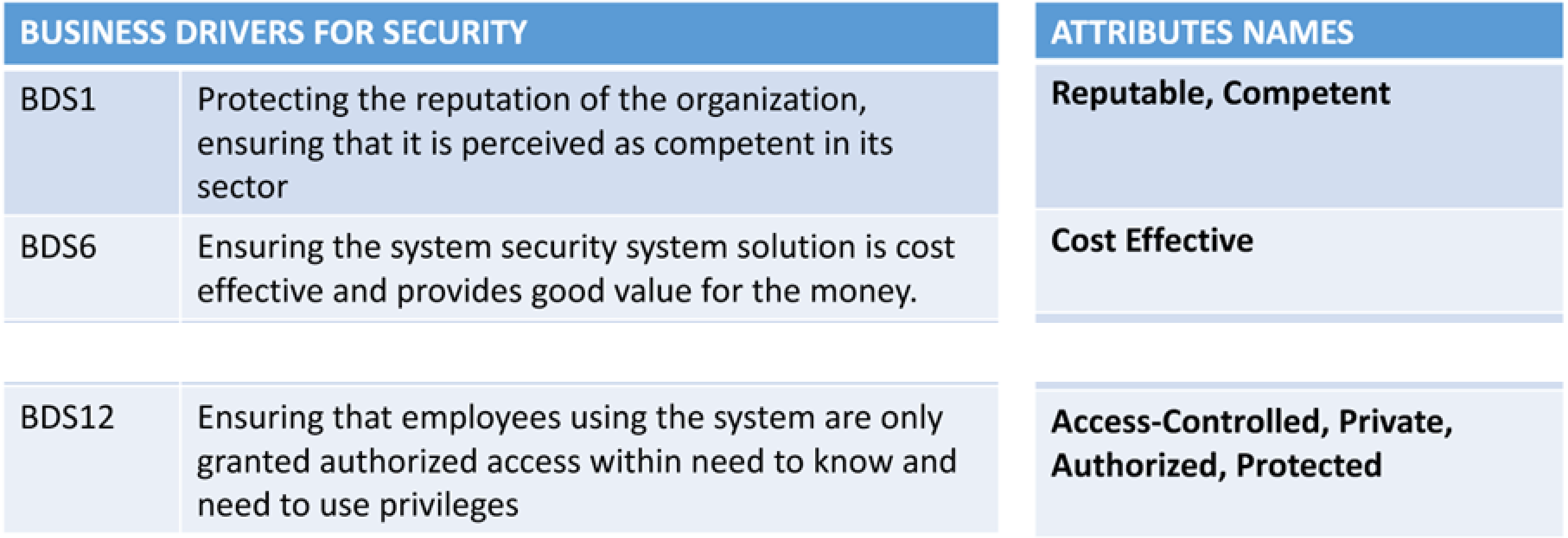
Sherwood applied business security architecture

- *What does this mean?*
- You interview the CFO, and ask, “What would be the impact of a data breach and the theft of our customer’s data?”, she states:
- “ABC Company’s reputation is critical for our business. If our customers loose faith in us, it would be detrimental to our growth. We collect a lot of sensitive personal information. I need a security solution that provides value for our spend and reduces our risk effectively. Given the current financial climate I can’t afford to spend a great deal. Specifically, I need to be able to ensure that user access is controlled and my people only have access to the functions and data they need.”

Sherwood applied business security architecture

- *What does this mean?*
- You interview the CFO, she states:
- **"ABC Company's reputation is critical for our business. If our customers loose faith in us, it would be detrimental to our growth.** We collect a lot of sensitive personal information. **I need a security solution that provides value for our spend and reduces our risk.** Given the current financial climate I can't afford to spend a great deal. **Specifically, I need to be able to ensure that user access is controlled and my people only have access to the functions and data they need.**"

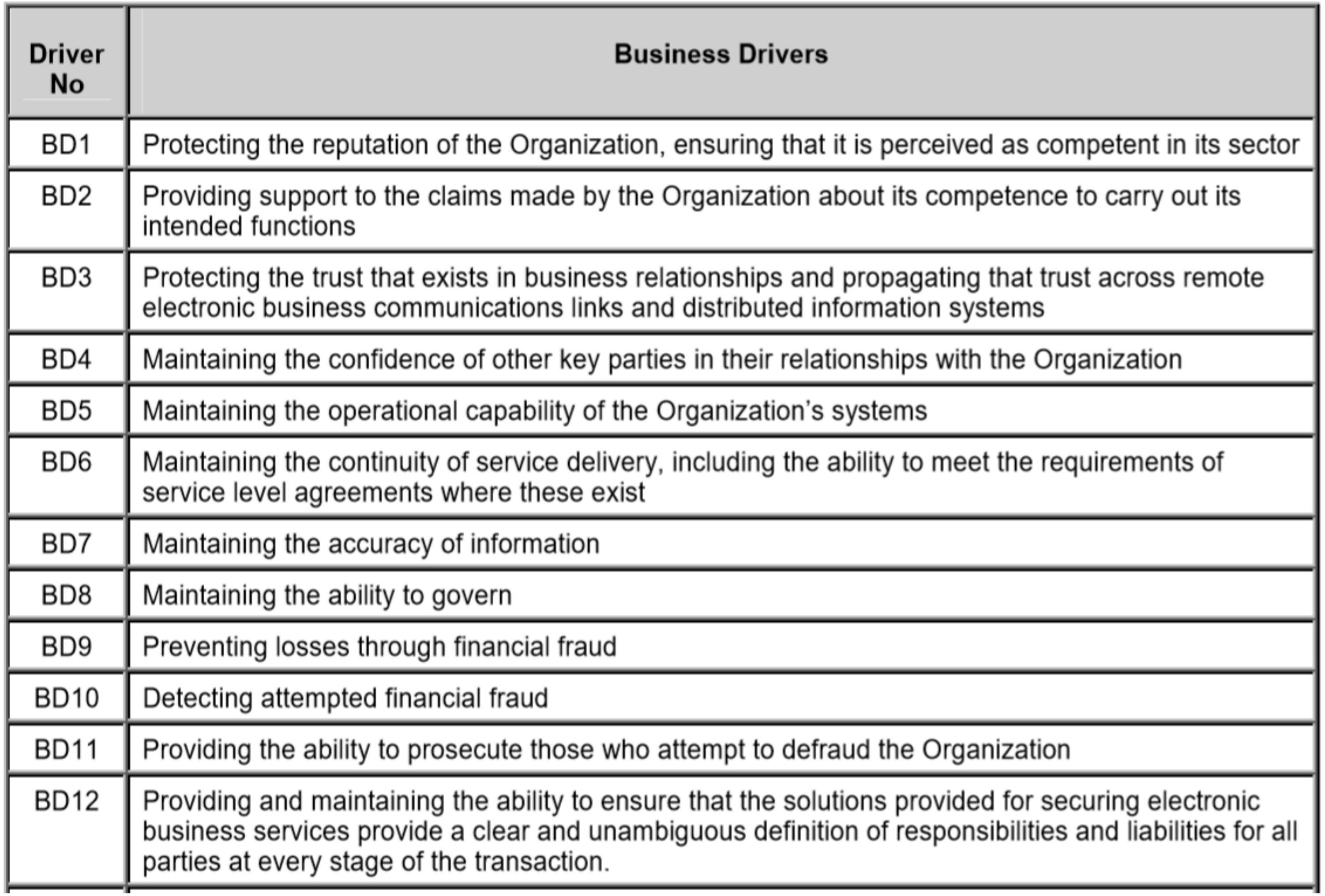
Sherwood applied business security architecture



BUSINESS DRIVERS FOR SECURITY		ATTRIBUTES NAMES
BDS1	Protecting the reputation of the organization, ensuring that it is perceived as competent in its sector	**Reputable, Competent**
BDS6	Ensuring the system security system solution is cost effective and provides good value for the money.	**Cost Effective**
BDS12	Ensuring that employees using the system are only granted authorized access within need to know and need to use privileges	**Access-Controlled, Private, Authorized, Protected**

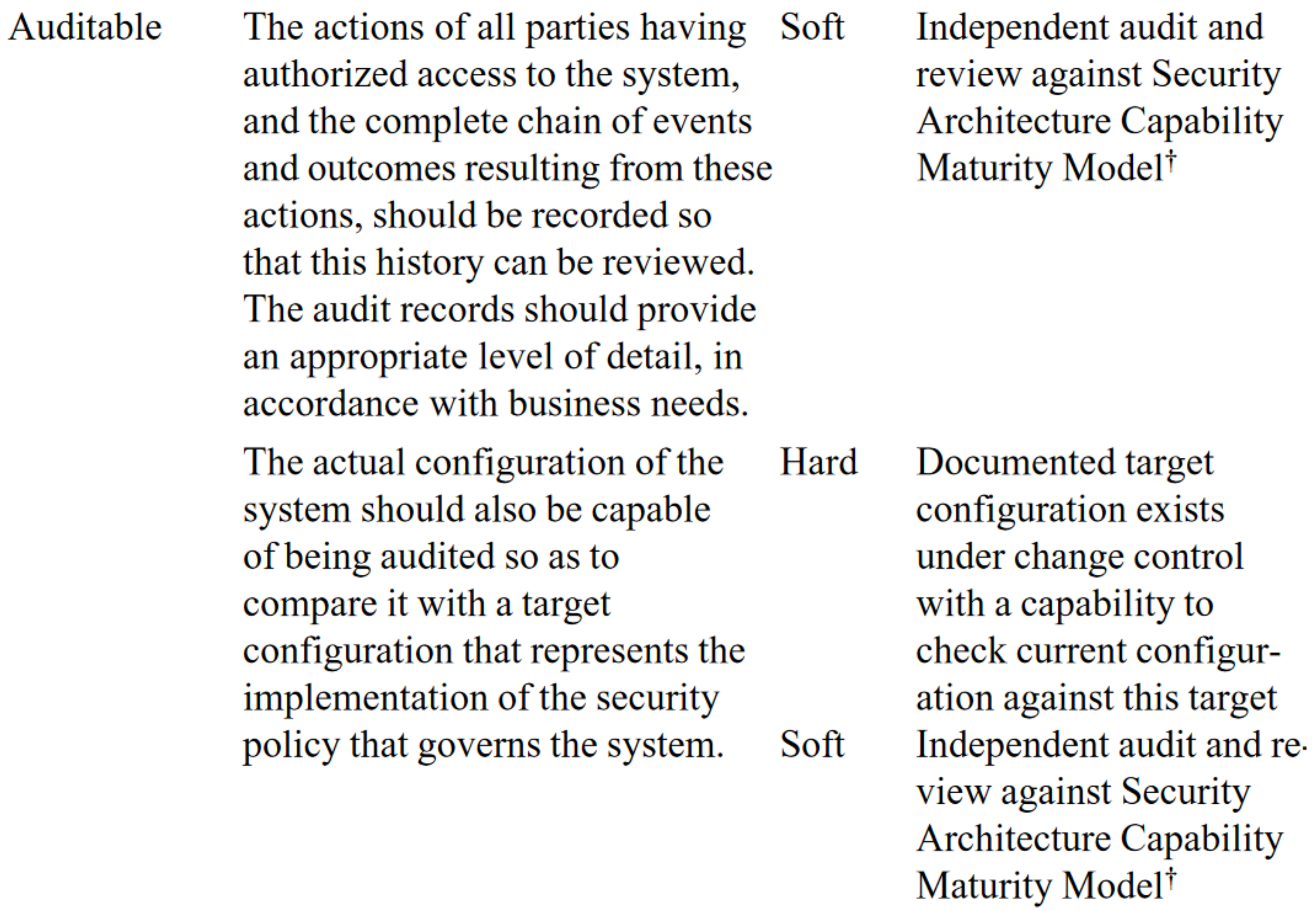
Source: David Lynas Consulting
https://sacramento.iiba.org/sites/sacramento/files/Events/201709/Introduction%20to%20SABSA%20for%20BAs%20-%20Sac%20Valley%20IIBA%2009.20.17%20FINAL.pdf

Sherwood applied business security architecture



Driver No	Business Drivers
BD1	Protecting the reputation of the Organization, ensuring that it is perceived as competent in its sector
BD2	Providing support to the claims made by the Organization about its competence to carry out its intended functions
BD3	Protecting the trust that exists in business relationships and propagating that trust across remote electronic business communications links and distributed information systems
BD4	Maintaining the confidence of other key parties in their relationships with the Organization
BD5	Maintaining the operational capability of the Organization's systems
BD6	Maintaining the continuity of service delivery, including the ability to meet the requirements of service level agreements where these exist
BD7	Maintaining the accuracy of information
BD8	Maintaining the ability to govern
BD9	Preventing losses through financial fraud
BD10	Detecting attempted financial fraud
BD11	Providing the ability to prosecute those who attempt to defraud the Organization
BD12	Providing and maintaining the ability to ensure that the solutions provided for securing electronic business services provide a clear and unambiguous definition of responsibilities and liabilities for all parties at every stage of the transaction.

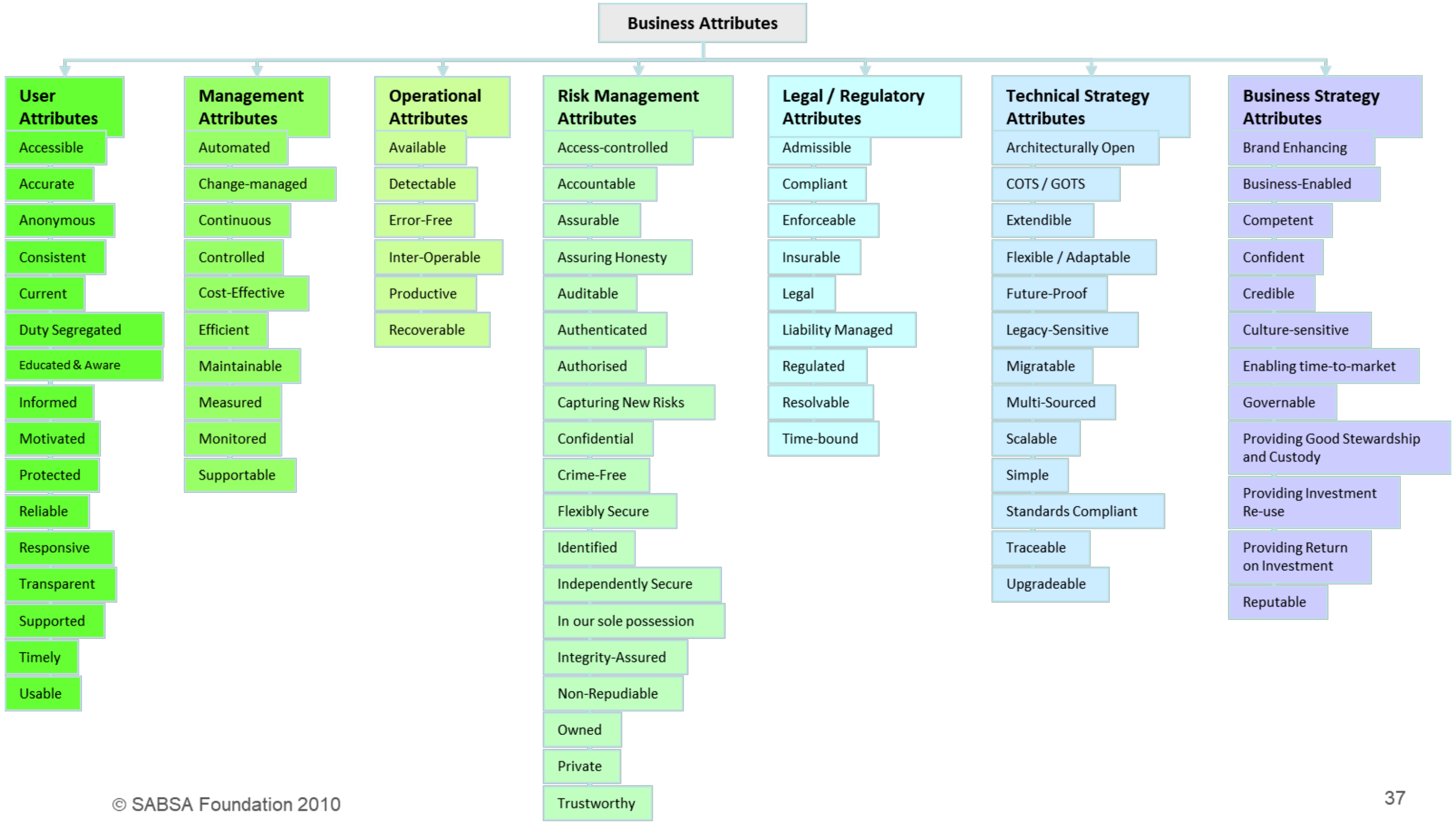
Sherwood applied business security architecture



Auditable	The actions of all parties having authorized access to the system, and the complete chain of events and outcomes resulting from these actions, should be recorded so that this history can be reviewed. The audit records should provide an appropriate level of detail, in accordance with business needs.	Soft	Independent audit and review against Security Architecture Capability Maturity Model†
	The actual configuration of the system should also be capable of being audited so as to compare it with a target configuration that represents the implementation of the security policy that governs the system.	Hard	Documented target configuration exists under change control with a capability to check current configuration against this target
		Soft	Independent audit and review against Security Architecture Capability Maturity Model†

Source: David Lynas Consulting
https://sacramento.iiba.org/sites/sacramento/files/Events/201709/Introduction%20to%20SABSA%20for%20BAs%20-%20Sac%20Valley%20IIBA%2009.20.17%20FINAL.pdf

Sherwood applied business security architecture



Business Attributes

User Attributes
- Accessible
- Accurate
- Anonymous
- Consistent
- Current
- Duty Segregated
- Educated & Aware
- Informed
- Motivated
- Protected
- Reliable
- Responsive
- Transparent
- Supported
- Timely
- Usable

Management Attributes
- Automated
- Change-managed
- Continuous
- Controlled
- Cost-Effective
- Efficient
- Maintainable
- Measured
- Monitored
- Supportable

Operational Attributes
- Available
- Detectable
- Error-Free
- Inter-Operable
- Productive
- Recoverable

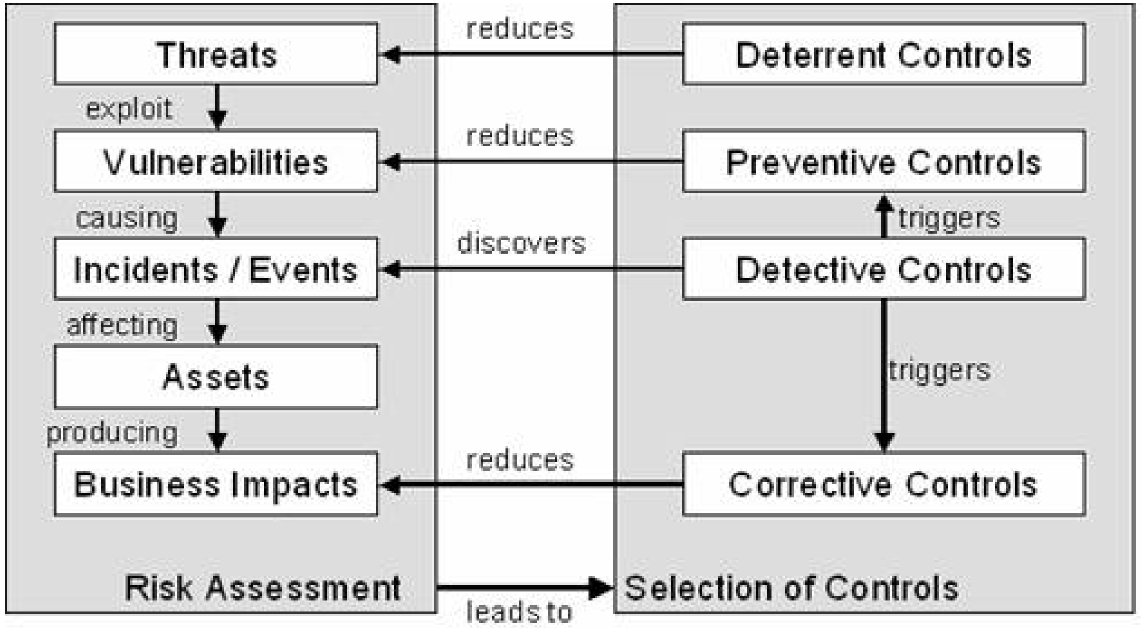
Risk Management Attributes
- Access-controlled
- Accountable
- Assurable
- Assuring Honesty
- Auditable
- Authenticated
- Authorised
- Capturing New Risks
- Confidential
- Crime-Free
- Flexibly Secure
- Identified
- Independently Secure
- In our sole possession
- Integrity-Assured
- Non-Repudiable
- Owned
- Private
- Trustworthy

Legal / Regulatory Attributes
- Admissible
- Compliant
- Enforceable
- Insurable
- Legal
- Liability Managed
- Regulated
- Resolvable
- Time-bound

Technical Strategy Attributes
- Architecturally Open
- COTS / GOTS
- Extendible
- Flexible / Adaptable
- Future-Proof
- Legacy-Sensitive
- Migratable
- Multi-Sourced
- Scalable
- Simple
- Standards Compliant
- Traceable
- Upgradeable

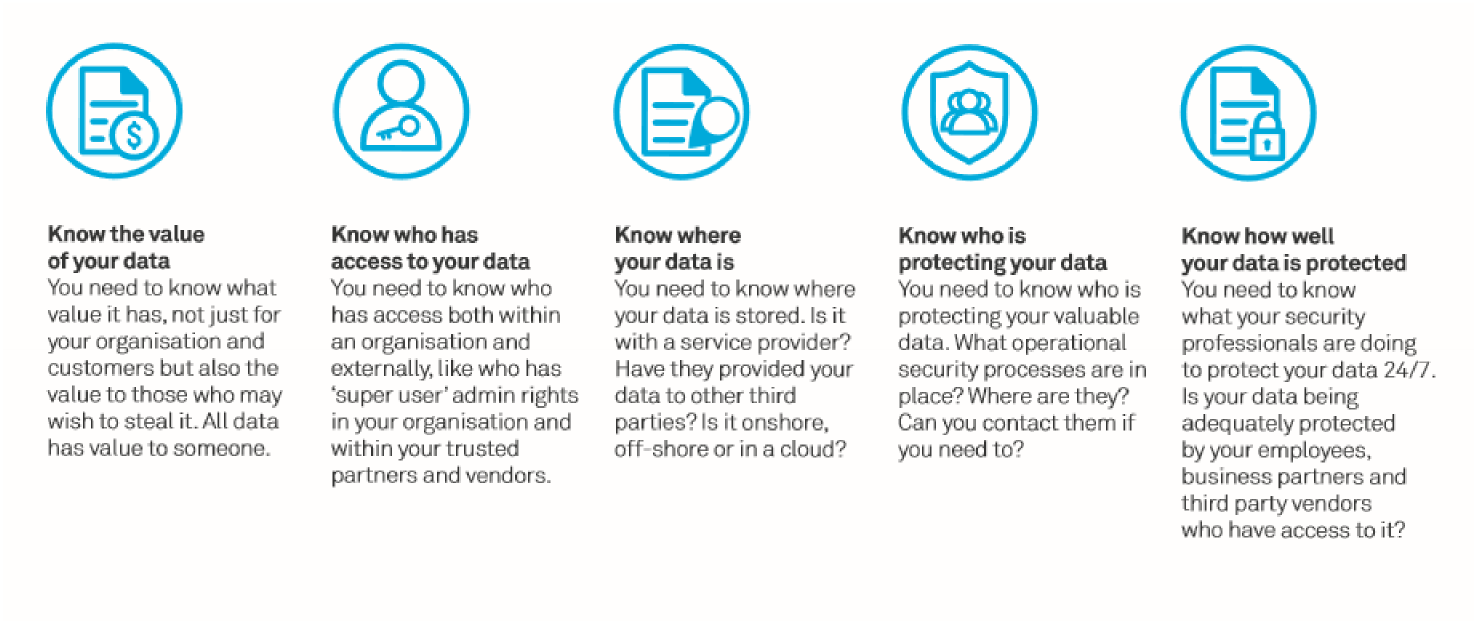
Business Strategy Attributes
- Brand Enhancing
- Business-Enabled
- Competent
- Confident
- Credible
- Culture-sensitive
- Enabling time-to-market
- Governable
- Providing Good Stewardship and Custody
- Providing Investment Re-use
- Providing Return on Investment
- Reputable

CONTROL SELECTION



Source: Sabsa

The five knows



Know the value of your data
You need to know what value it has, not just for your organisation and customers but also the value to those who may wish to steal it. All data has value to someone.

Know who has access to your data
You need to know who has access both within an organisation and externally, like who has 'super user' admin rights in your organisation and within your trusted partners and vendors.

Know where your data is
You need to know where your data is stored. Is it with a service provider? Have they provided your data to other third parties? Is it onshore, off-shore or in a cloud?

Know who is protecting your data
You need to know who is protecting your valuable data. What operational security processes are in place? Where are they? Can you contact them if you need to?

Know how well your data is protected
You need to know what your security professionals are doing to protect your data 24/7. Is your data being adequately protected by your employees, business partners and third party vendors who have access to it?

Source: https://www.telstra.com.au/business-enterprise/solutions/security/security-services

Threat Agent Risk Assessment (TARA)

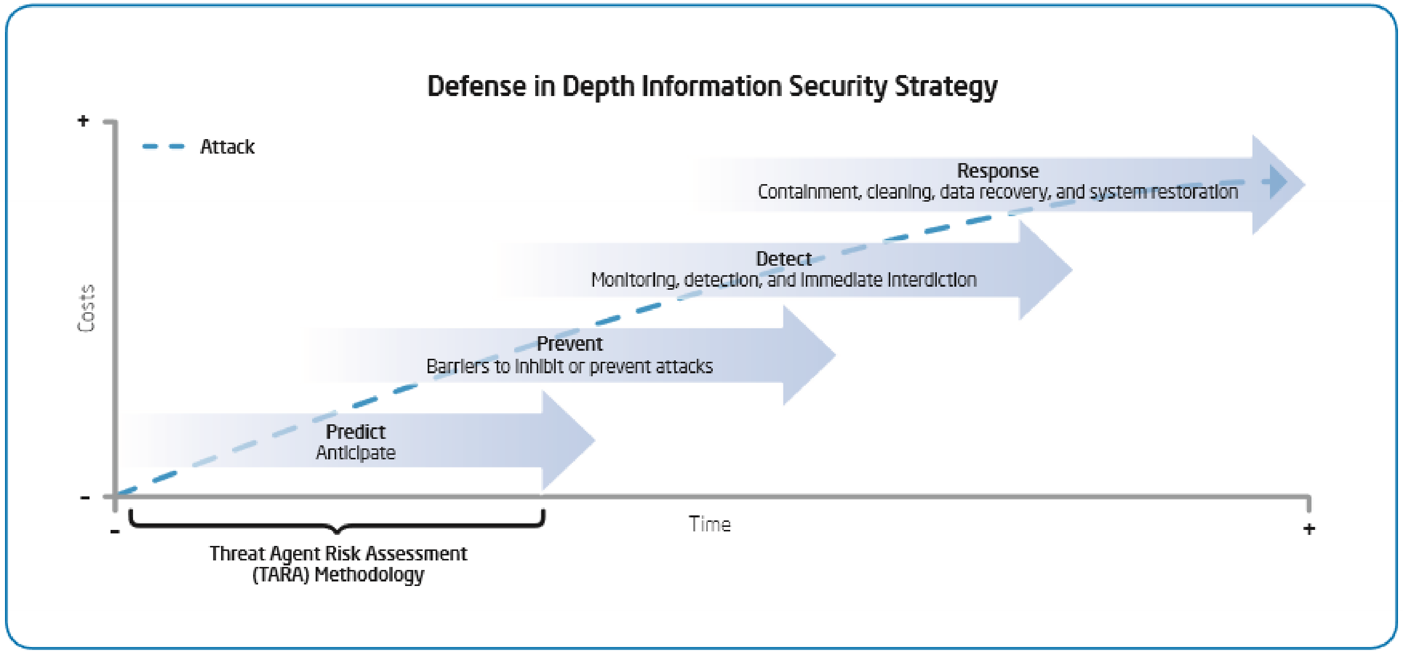

Defense in Depth Information Security Strategy
+
Attack
Costs
-
Response
Containment, cleaning, data recovery, and system restoration
Detect
Monitoring, detection, and immediate interdiction
Prevent
Barriers to inhibit or prevent attacks
Predict
Anticipate
-
Time
+
Threat Agent Risk Assessment
(TARA) Methodology

Figure 1. The threat agent risk assessment (TARA) methodology fits into the predict phase of our defense in depth information security strategy.

Source: https://itpeernetwork.intel.com/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment/

Threat agent risk assessment

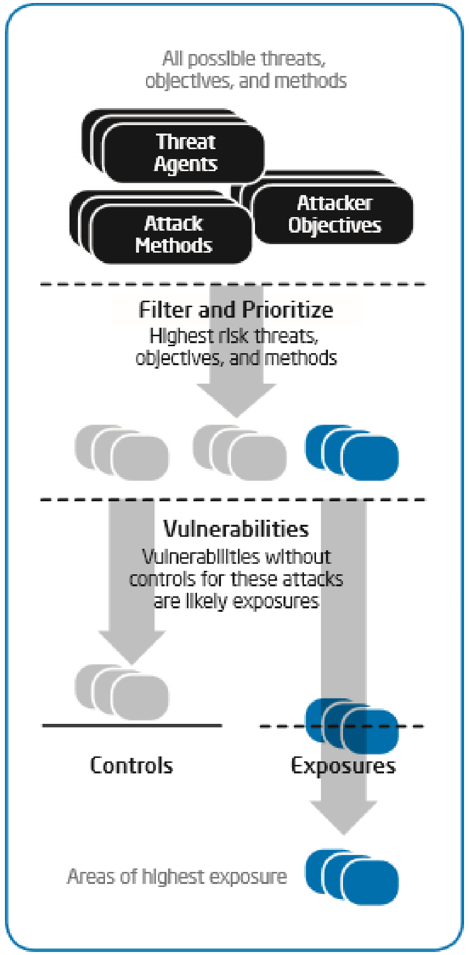
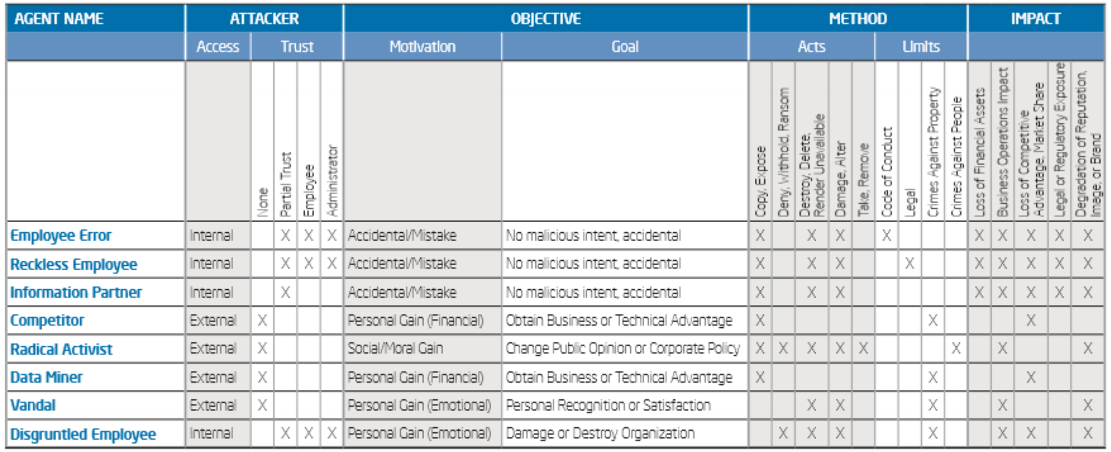


Figure 2. The threat agent risk assessment (TARA) methodology narrows the field of all possible attacks to determine the most likely attacks.

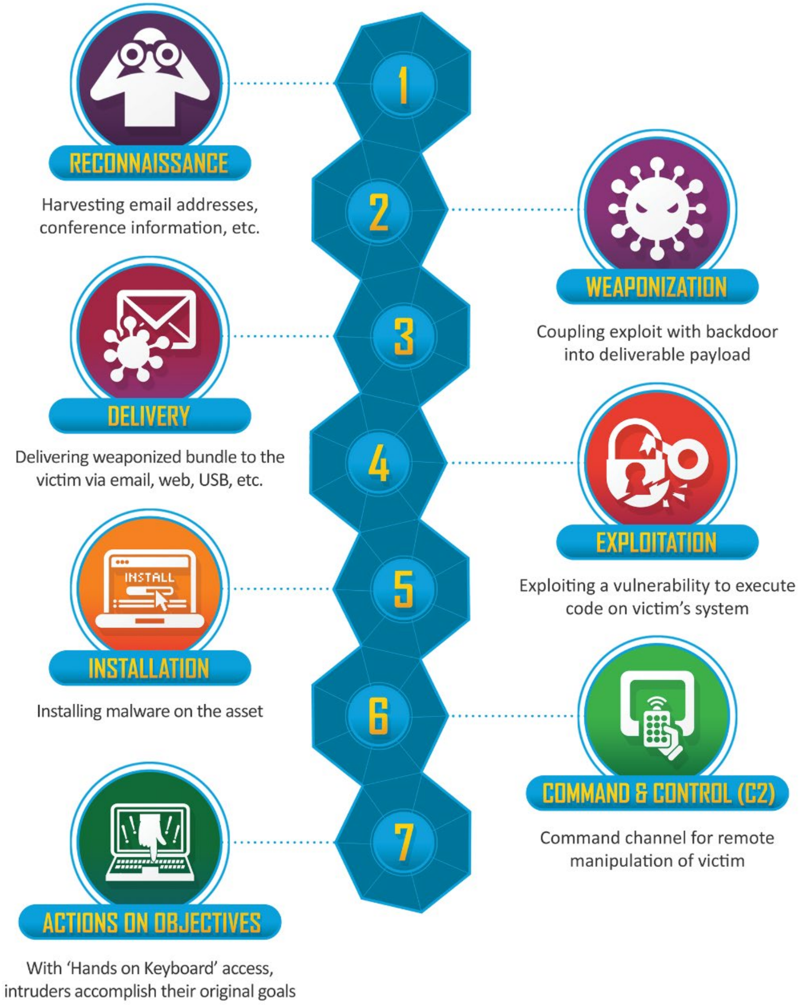
Table 1. Sample from Methods and Objectives (MOL) Library



AGENT NAME	ATTACKER					OBJECTIVE		METHOD									IMPACT				
	Access	Trust				Motivation	Goal	Acts					Limits								
		None	Partial Trust	Employee	Administrator			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of Conduct	Legal	Crimes Against Property	Crimes Against People	Loss of Financial Assets	Business Operations Impact	Loss of Competitive Advantage, Market Share	Legal or Regulatory Exposure	Degradation of Reputation, Image, or Brand
Employee Error	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X		X				X	X	X	X	X
Reckless Employee	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X			X			X	X	X	X	X
Information Partner	Internal		X			Accidental/Mistake	No malicious intent, accidental	X		X	X						X	X	X	X	X
Competitor	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Radical Activist	External	X				Social/Moral Gain	Change Public Opinion or Corporate Policy	X	X	X	X	X				X		X			X
Data Miner	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Vandal	External	X				Personal Gain (Emotional)	Personal Recognition or Satisfaction			X	X				X			X			X
Disgruntled Employee	Internal		X	X	X	Personal Gain (Emotional)	Damage or Destroy Organization		X	X	X				X			X	X		X

Source: https://itpeernetwork.intel.com/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment/

Lockheed Martin cyber kill chain



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Source: https://lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Verizon Data Breach Investigations Report (VDIR)

2019 Data Breach Investigations Report

verizon✓
business ready

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report (VDIR)

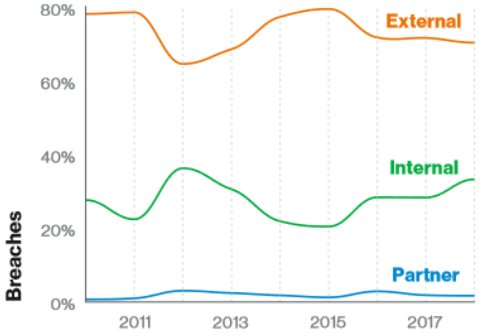


Figure 6. Threat actors in breaches over time

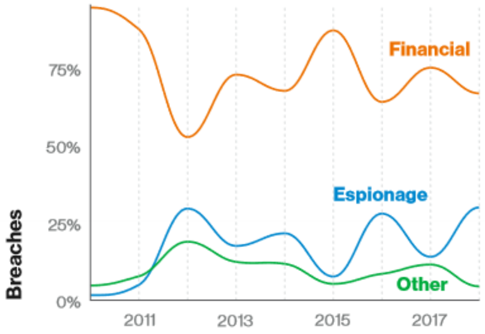


Figure 7. Threat actor motives in breaches over time

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report (VDIR)

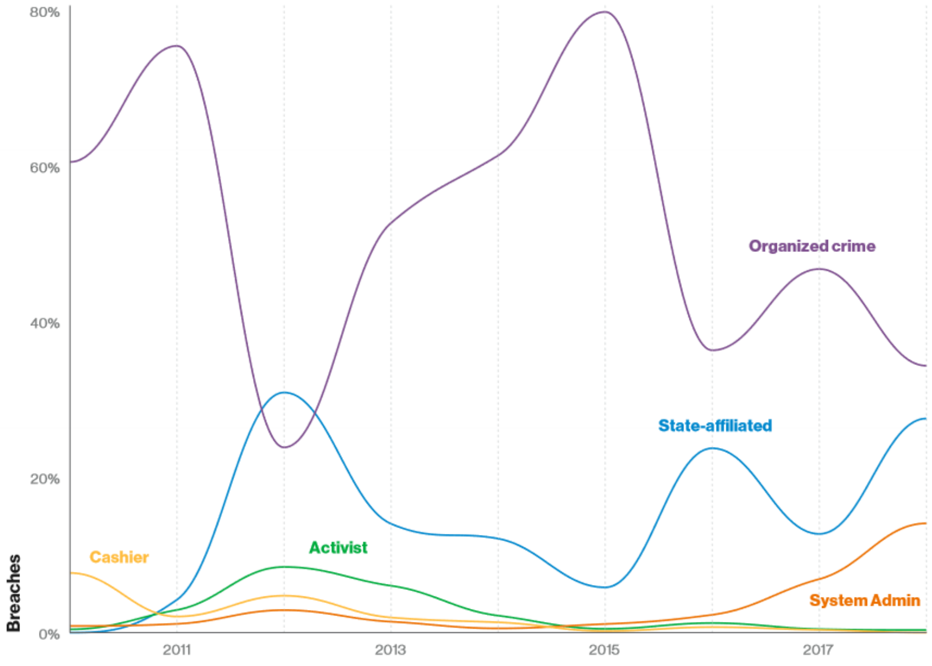


Figure 8. Select threat actors in breaches over time

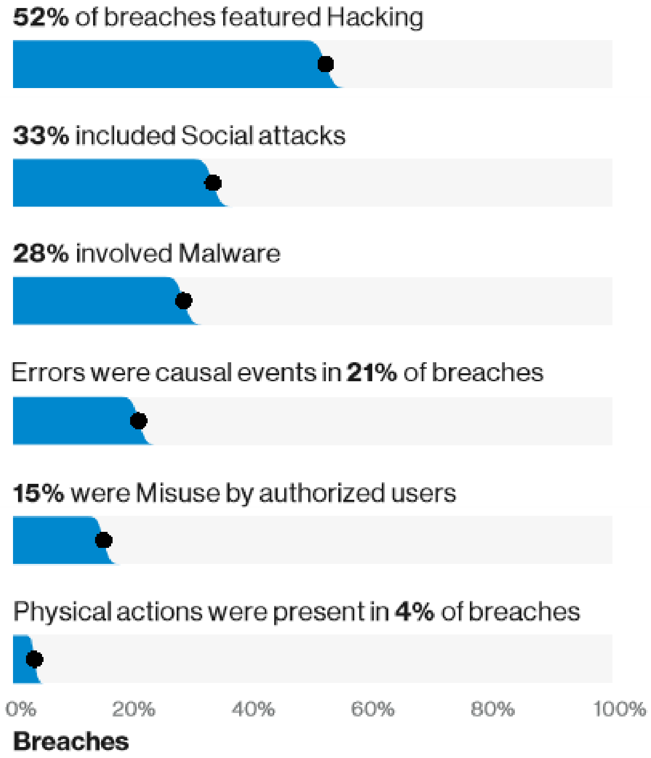


Figure 3. What tactics are utilized?

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report

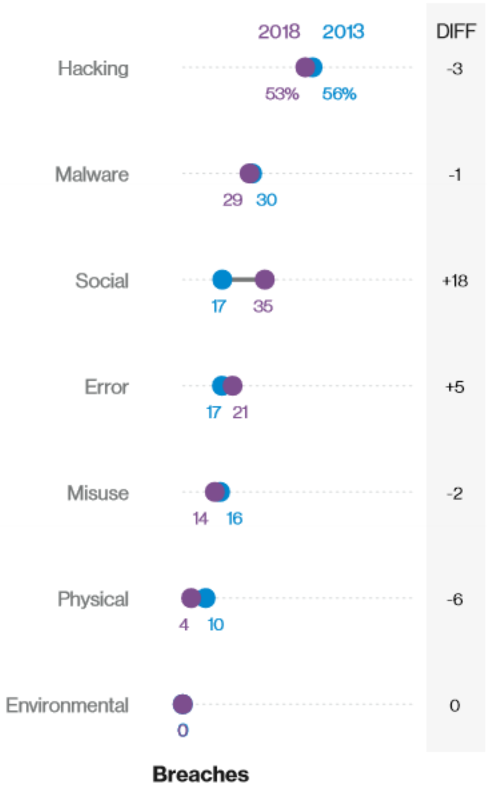


Figure 9. Threat actions in data breaches over time
n=2,501 (2013), n=1,638 (2018)

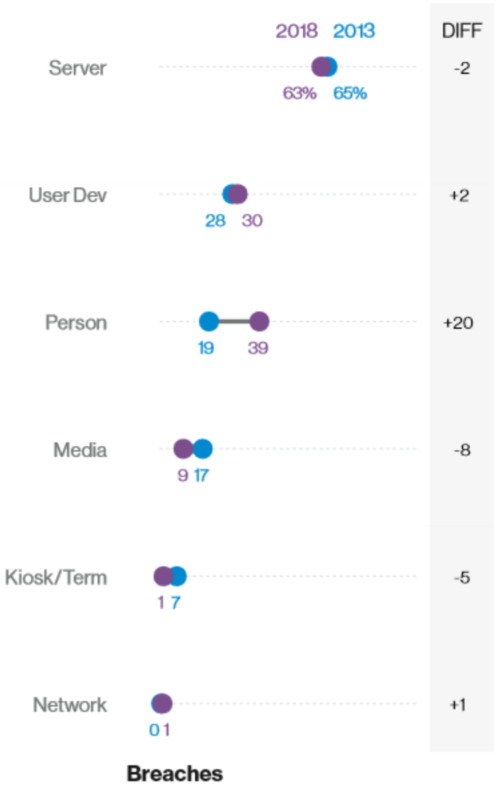
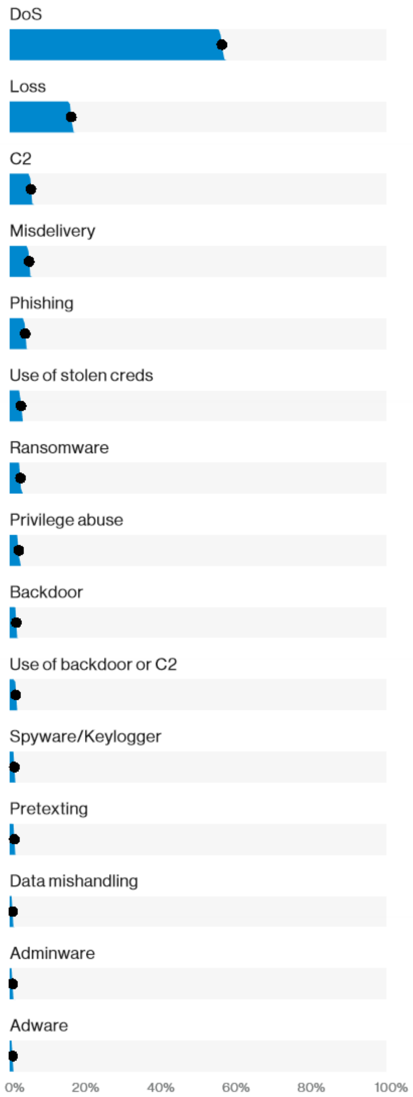


Figure 10. Asset categories in data breaches over time
n=2,294 (2013), n=1,513 (2018)

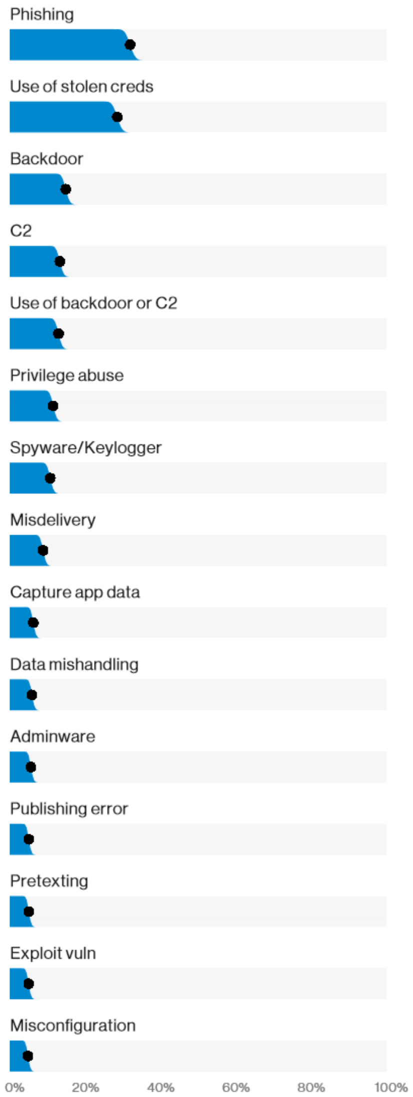
Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report (VDIR)



Incidents

Figure 11. Top threat action varieties in incidents, (n=17,310)



Breaches

Figure 12. Top threat action varieties in breaches (n=1,774)

Verizon Data Breach Investigations Report

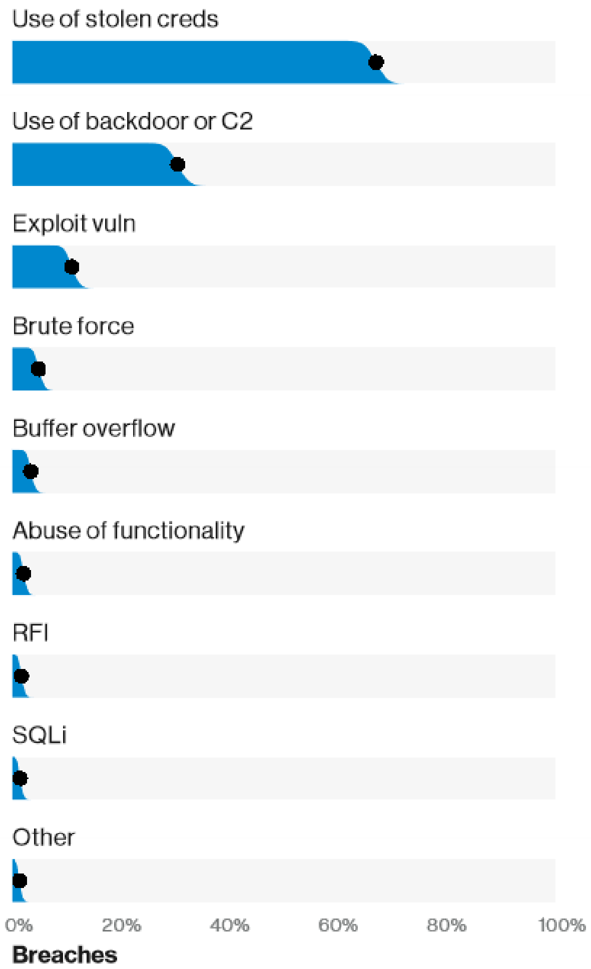


Figure 13. Top hacking action varieties in breaches (n=755)

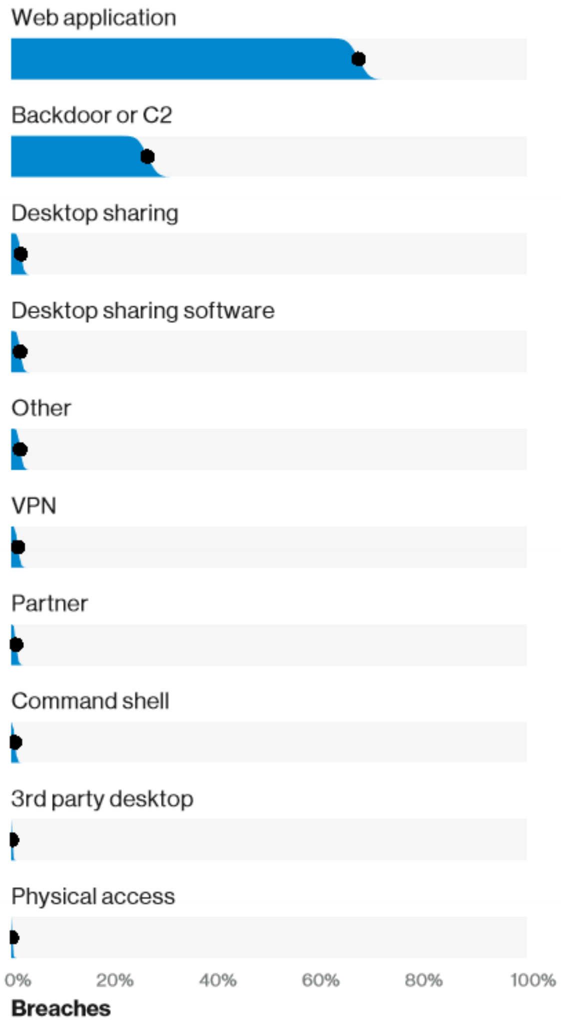


Figure 14. Top hacking action vectors in breaches (n=862)

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report

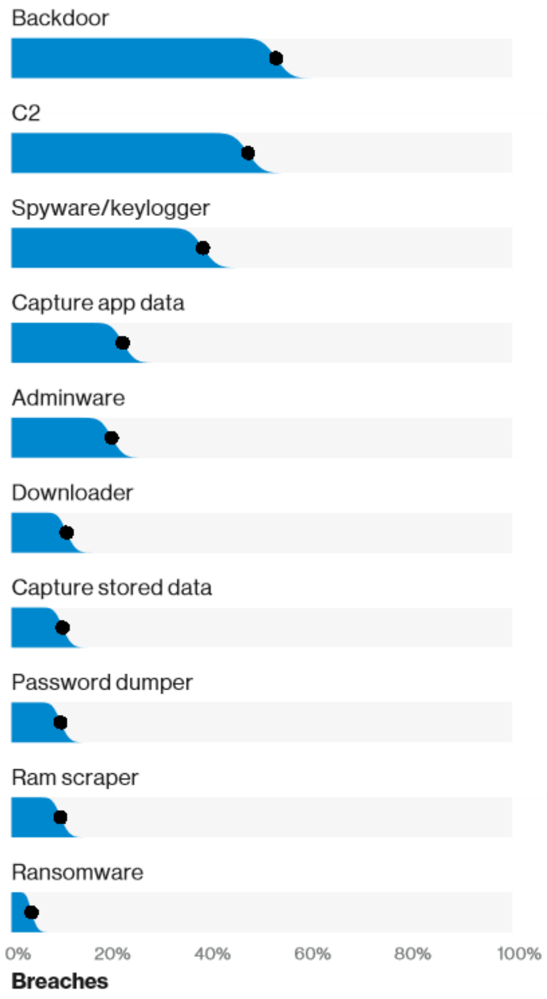


Figure 17. Top malware action varieties in breaches (n=500)

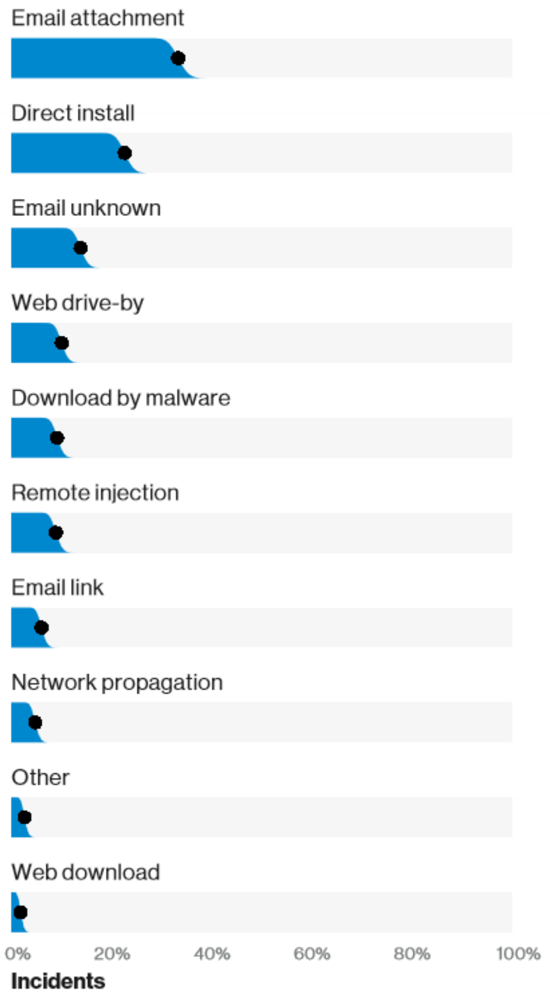


Figure 18. Top malware action vectors in incidents (n=795)

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report

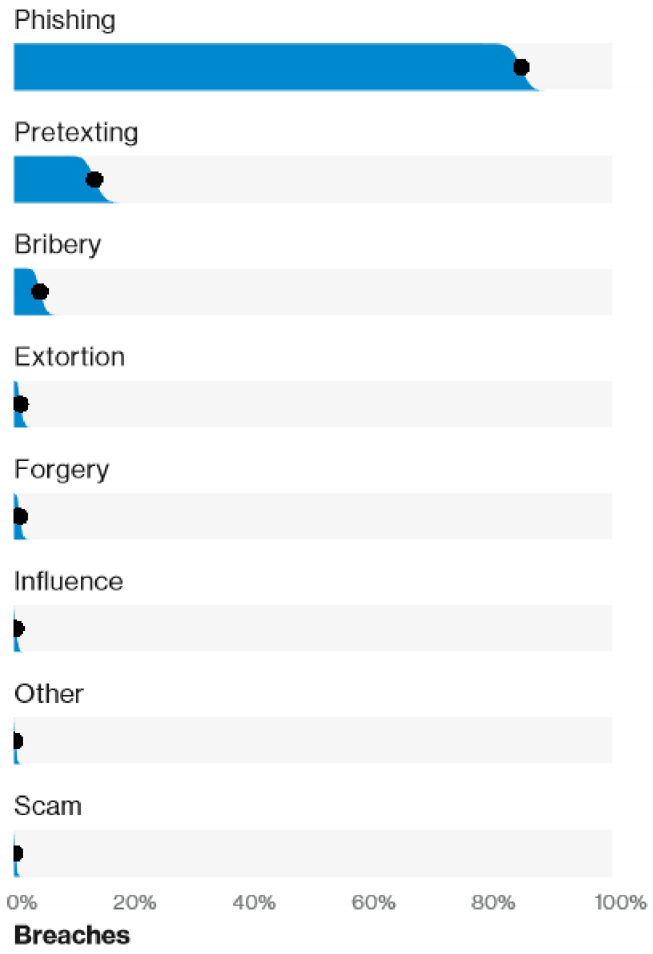


Figure 20. Top social action varieties in breaches (n=670)

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report

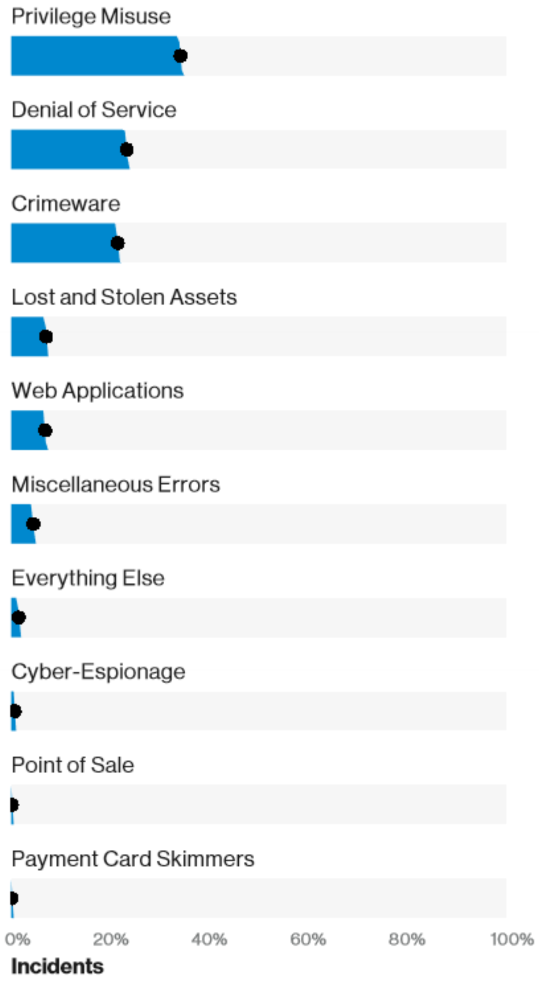


Figure 35. Incidents per pattern (n=41,686)

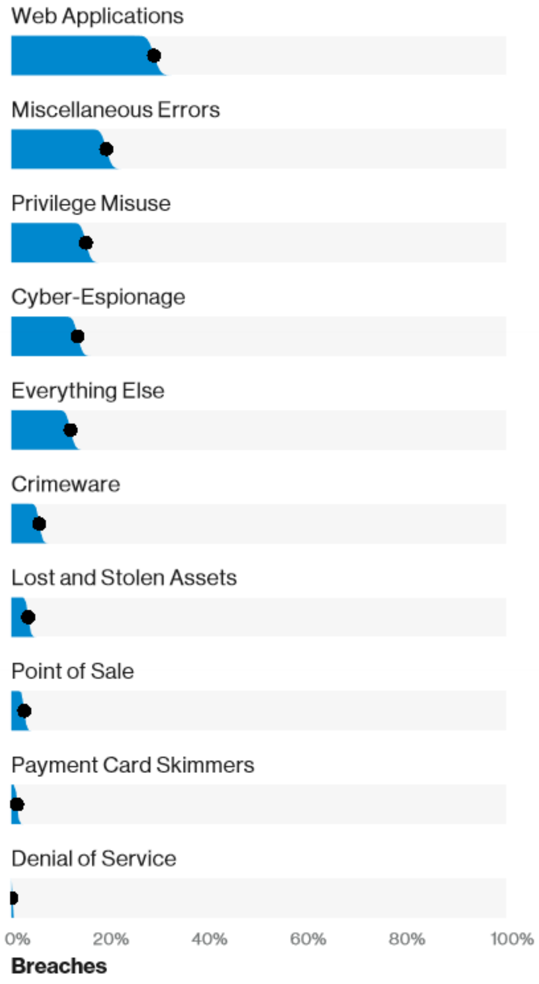
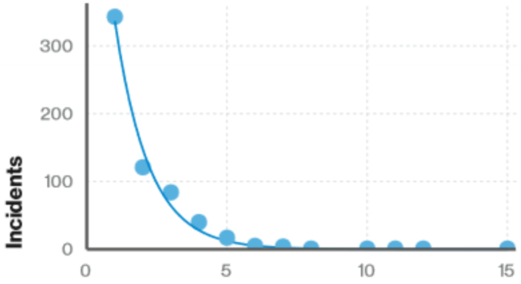


Figure 36. Breaches per pattern (n=2,013)

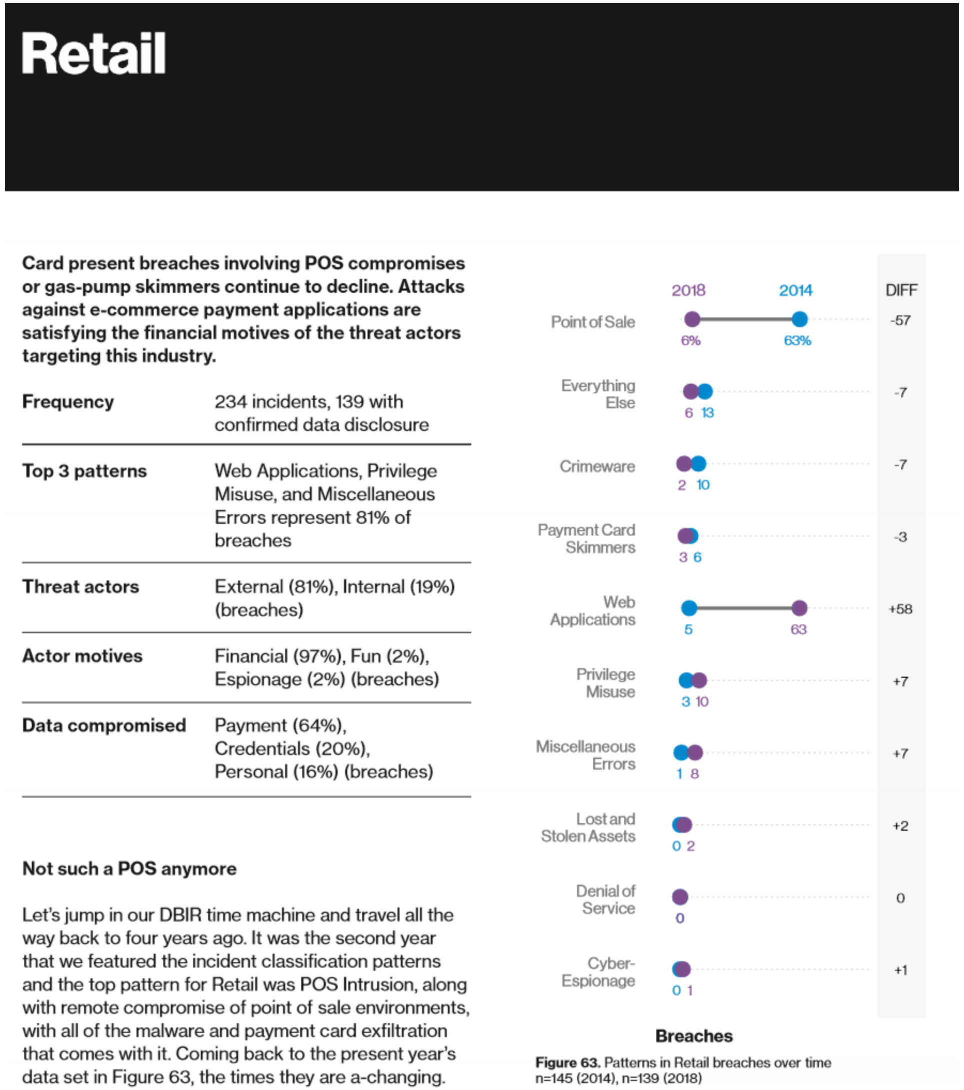
Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report



Number of steps

Figure 29. Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths.



Retail

Card present breaches involving POS compromises or gas-pump skimmers continue to decline. Attacks against e-commerce payment applications are satisfying the financial motives of the threat actors targeting this industry.

Frequency	234 incidents, 139 with confirmed data disclosure
Top 3 patterns	Web Applications, Privilege Misuse, and Miscellaneous Errors represent 81% of breaches
Threat actors	External (81%), Internal (19%) (breaches)
Actor motives	Financial (97%), Fun (2%), Espionage (2%) (breaches)
Data compromised	Payment (64%), Credentials (20%), Personal (16%) (breaches)

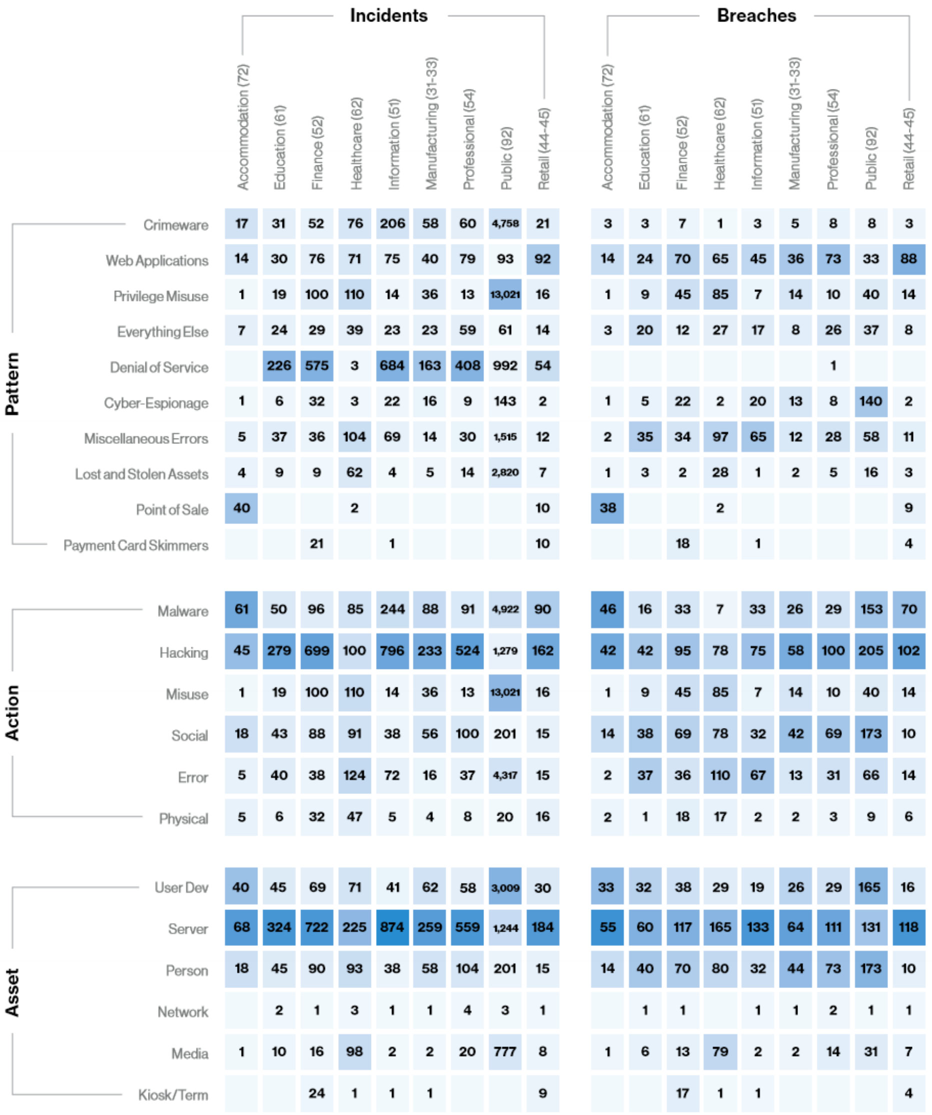
Not such a POS anymore

Let's jump in our DBIR time machine and travel all the way back to four years ago. It was the second year that we featured the incident classification patterns and the top pattern for Retail was POS Intrusion, along with remote compromise of point of sale environments, with all of the malware and payment card exfiltration that comes with it. Coming back to the present year's data set in Figure 63, the times they are a-changing.

Figure 63. Patterns in Retail breaches over time n=145 (2014), n=139 (2018)

Source: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Data Breach Investigations Report



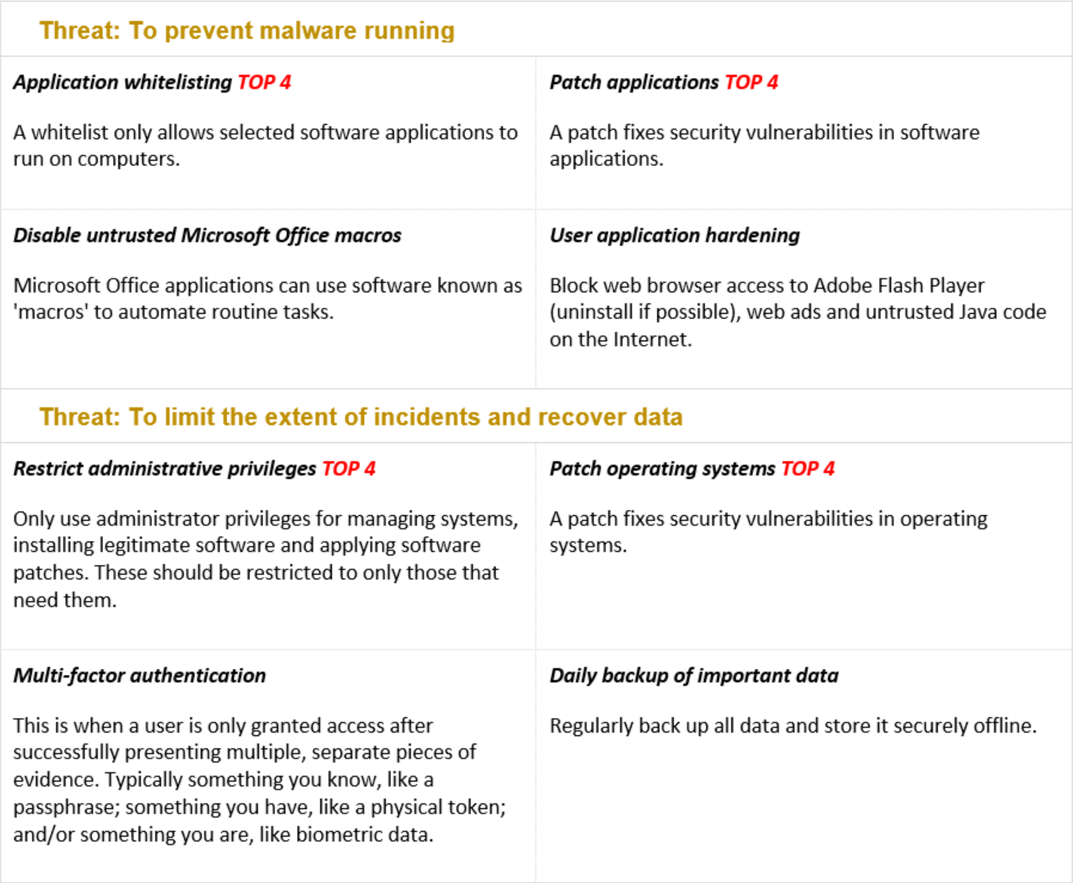
		Incidents									Breaches								
		Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Pattern	Crimeware	17	31	52	76	206	58	60	4,758	21	3	3	7	1	3	5	8	8	3
	Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
	Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
	Denial of Service		226	575	3	684	163	408	992	54							1		
	Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
	Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
	Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
	Point of Sale	40			2					10	38			2					9
	Payment Card Skimmers			21		1				10			18		1				4
Action	Malware	61	50	96	85	244	88	91	4,922	90	46	16	33	7	33	26	29	153	70
	Hacking	45	279	699	100	796	233	524	1,279	162	42	42	95	78	75	58	100	205	102
	Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Social	18	43	88	91	38	56	100	201	15	14	38	69	78	32	42	69	173	10
	Error	5	40	38	124	72	16	37	4,317	15	2	37	36	110	67	13	31	66	14
	Physical	5	6	32	47	5	4	8	20	16	2	1	18	17	2	2	3	9	6
Asset	User Dev	40	45	69	71	41	62	58	3,009	30	33	32	38	29	19	26	29	165	16
	Server	68	324	722	225	874	259	559	1,244	184	55	60	117	165	133	64	111	131	118
	Person	18	45	90	93	38	58	104	201	15	14	40	70	80	32	44	73	173	10
	Network		2	1	3	1	1	4	3	1		1	1		1	1	2	1	1
	Media	1	10	16	98	2	2	20	777	8	1	6	13	79	2	2	14	31	7
	Kiosk/Term			24	1	1	1			9			17	1	1				4

Figure 39. Industry Comparison
(left: all security incidents, right: only breaches)

0% 25% 50% 75% 100%

Source:
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

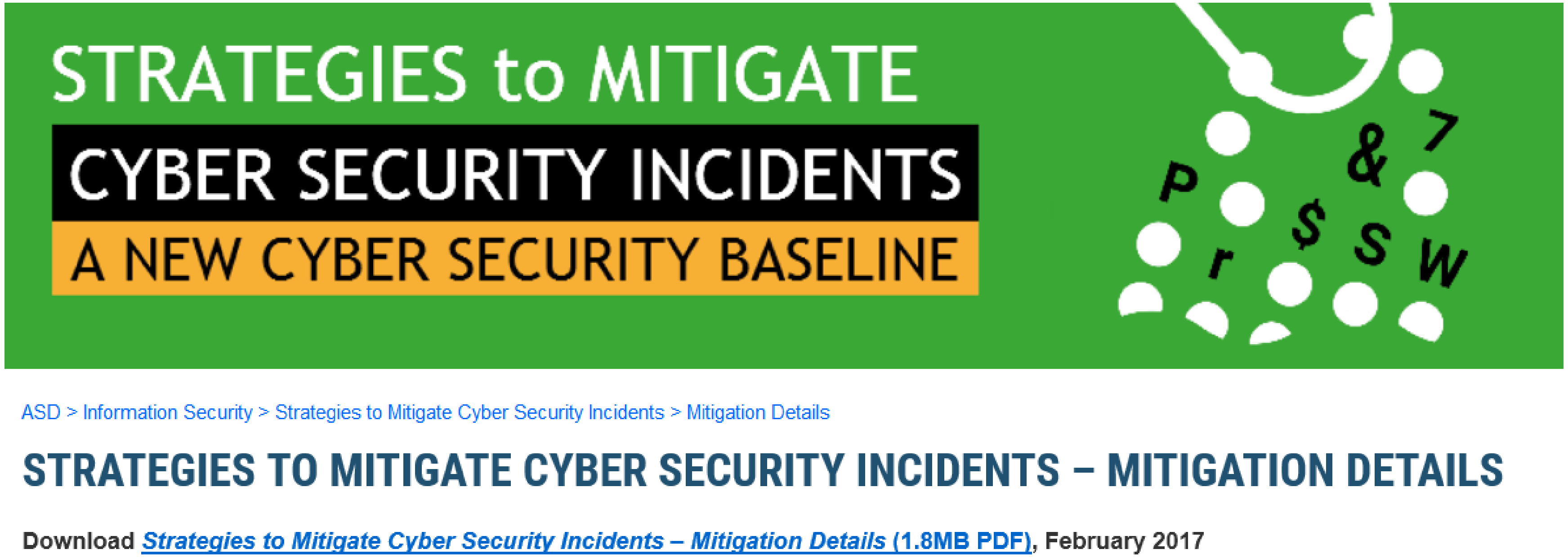
Australian Signals Directorate (ASD) ESSENTIAL 8



Threat: To prevent malware running	
Application whitelisting ***TOP 4*** A whitelist only allows selected software applications to run on computers.	***Patch applications*** ***TOP 4*** A patch fixes security vulnerabilities in software applications.
Disable untrusted Microsoft Office macros Microsoft Office applications can use software known as 'macros' to automate routine tasks.	***User application hardening*** Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet.
Threat: To limit the extent of incidents and recover data	
Restrict administrative privileges ***TOP 4*** Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them.	***Patch operating systems*** ***TOP 4*** A patch fixes security vulnerabilities in operating systems.
Multi-factor authentication This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically something you know, like a passphrase; something you have, like a physical token; and/or something you are, like biometric data.	***Daily backup of important data*** Regularly back up all data and store it securely offline.

- Source: https://www.cyber.gov.au/publications/essential -eight-explained

Australian Signals Directorate (ASD)



STRATEGIES to MITIGATE

CYBER SECURITY INCIDENTS

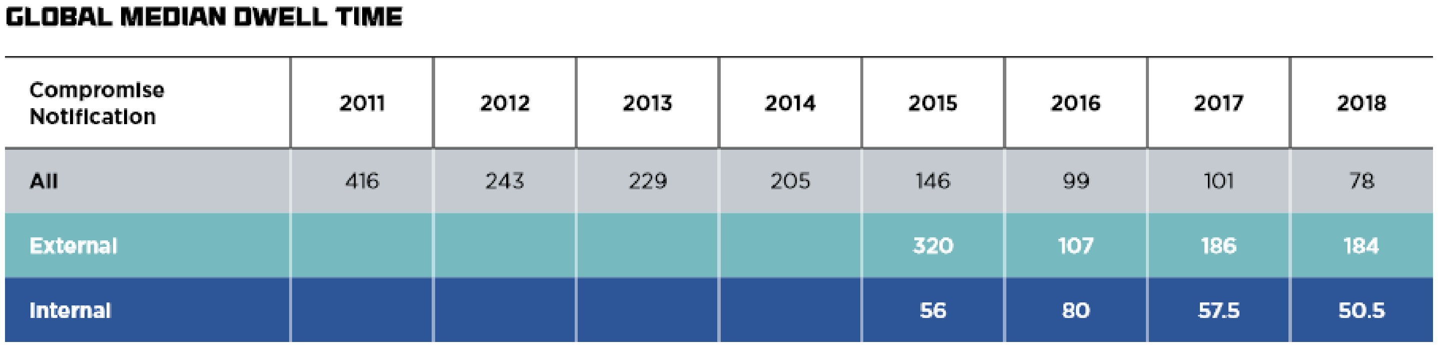
A NEW CYBER SECURITY BASELINE

ASD > Information Security > Strategies to Mitigate Cyber Security Incidents > Mitigation Details

STRATEGIES TO MITIGATE CYBER SECURITY INCIDENTS – MITIGATION DETAILS

Download ***Strategies to Mitigate Cyber Security Incidents – Mitigation Details* (1.8MB PDF)**, February 2017

Mandiant M-Trends Report



GLOBAL MEDIAN DWELL TIME

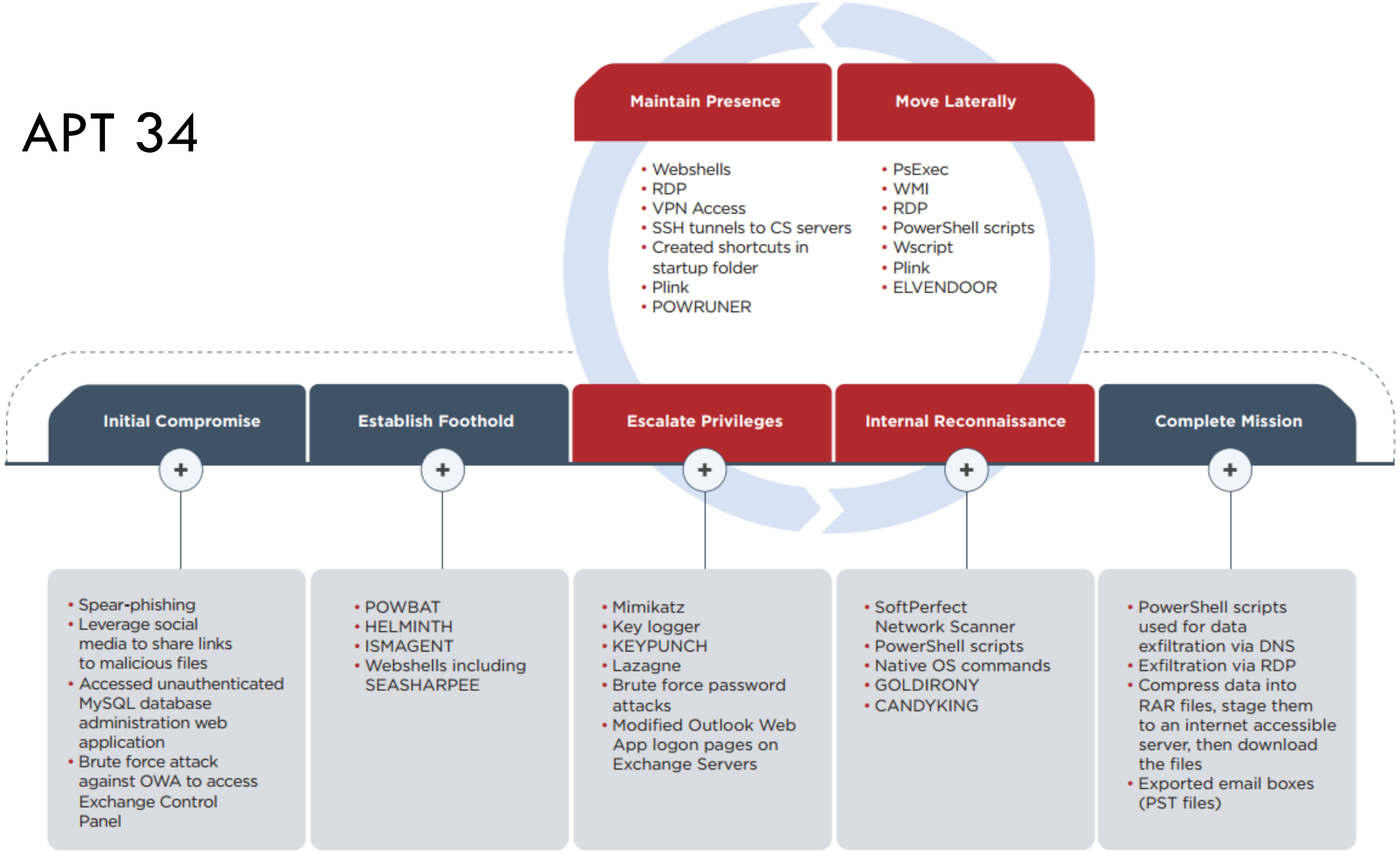
Compromise Notification	2011	2012	2013	2014	2015	2016	2017	2018
All	416	243	229	205	146	99	101	78
External					320	107	186	184
Internal					56	80	57.5	50.5

Mandiant M-Trends Report

- Security risk management
- Incident response
- Identity and access management
- Network, cloud and data center protection
- Data protection
- Host and endpoint protection

Mandiant M-Trends Report

APT 34



Maintain Presence

- Webshells
- RDP
- VPN Access
- SSH tunnels to CS servers
- Created shortcuts in startup folder
- Plink
- POWRUNER

Move Laterally

- PsExec
- WMI
- RDP
- PowerShell scripts
- Wscript
- Plink
- ELVENDOOR

Initial Compromise

- Spear-phishing
- Leverage social media to share links to malicious files
- Accessed unauthenticated MySQL database administration web application
- Brute force attack against OWA to access Exchange Control Panel

Establish Foothold

- POWBAT
- HELMINTH
- ISMAGENT
- Webshells including SEASHARPEE

Escalate Privileges

- Mimikatz
- Key logger
- KEYPUNCH
- Lazagne
- Brute force password attacks
- Modified Outlook Web App logon pages on Exchange Servers

Internal Reconnaissance

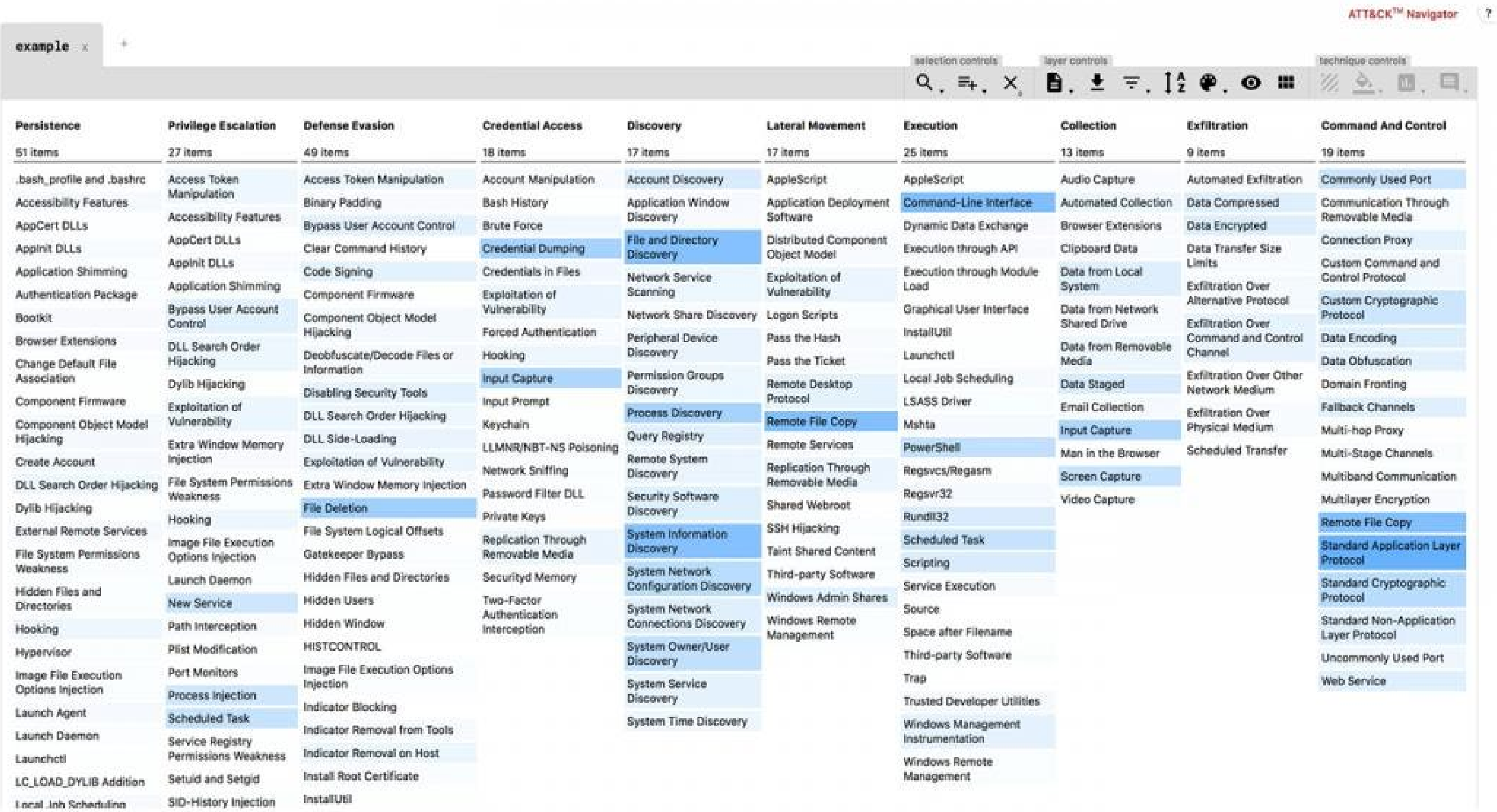
- SoftPerfect Network Scanner
- PowerShell scripts
- Native OS commands
- GOLDIRONY
- CANDYKING

Complete Mission

- PowerShell scripts used for data exfiltration via DNS
- Exfiltration via RDP
- Compress data into RAR files, stage them to an internet accessible server, then download the files
- Exported email boxes (PST files)

Source: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

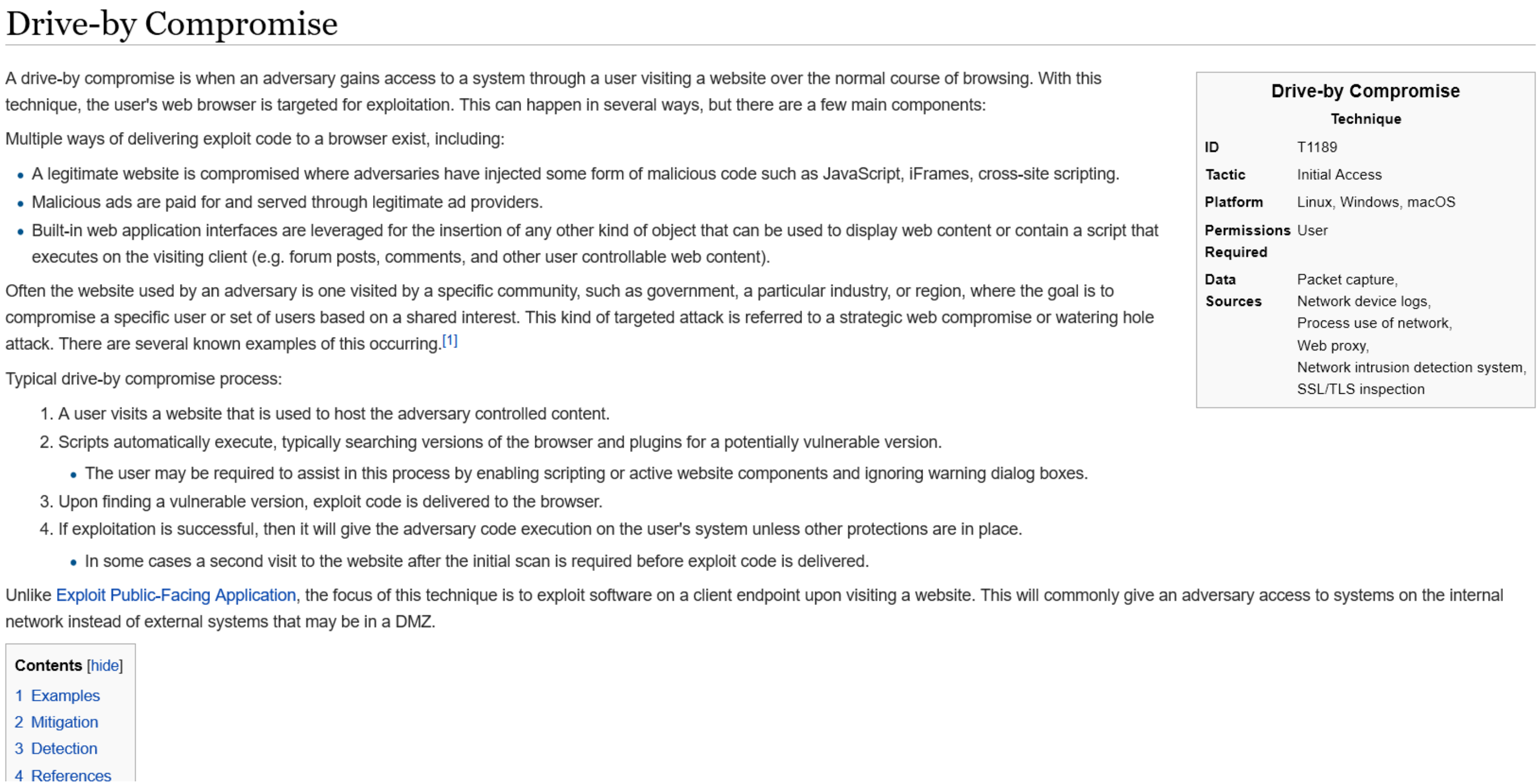
Mitre Adversarial Tactics, Techniques & Common Knowledge (ATTACK)



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command And Control
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items	19 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Hooking	Process Discovery	Remote Desktop Protocol	Launchctl	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Capture	Query Registry	Remote File Copy	Local Job Scheduling	Email Collection	Scheduled Transfer	Fallback Channels
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Input Prompt	Remote System Discovery	Remote Services	LSASS Driver	Input Capture		Multi-hop Proxy
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser		Multi-Stage Channels
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	Shared Webroot	PowerShell	Screen Capture		Multiband Communication
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Regsvcs/Regasm	Video Capture		Multilayer Encryption
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32			Remote File Copy
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32			Standard Application Layer Protocol
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media	System Service Discovery	Windows Admin Shares	Scheduled Task			Standard Cryptographic Protocol
Hidden Files and Directories	Plist Modification	Hidden Files and Directories	Securityd Memory	System Time Discovery	Windows Remote Management	Scripting			Standard Non-Application Layer Protocol
Hooking	Port Monitors	Hidden Users	Two-Factor Authentication Interception			Service Execution			Uncommonly Used Port
Hypervisor	Process Injection	Hidden Window				Source			Web Service
Image File Execution Options Injection	Scheduled Task	HISTCONTROL				Space after Filename			
Launch Agent	Service Registry Permissions Weakness	Image File Execution Options Injection				Third-party Software			
Launch Daemon	Setuid and Setgid	Indicator Blocking				Trap			
Launchctl	SID-History Injection	Indicator Removal from Tools				Trusted Developer Utilities			
LC_LOAD_DYLIB Addition		Indicator Removal on Host				Windows Management Instrumentation			
Local Job Scheduling		Install Root Certificate				Windows Remote Management			
		InstallUtil							

Source: https://attack.mitre.org/wiki/Main_Page

Mitre Adversarial Tactics, Techniques & Common Knowledge (ATTACK)



Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.[1]

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
   - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
   - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike Exploit Public-Facing Application, the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

Drive-by Compromise

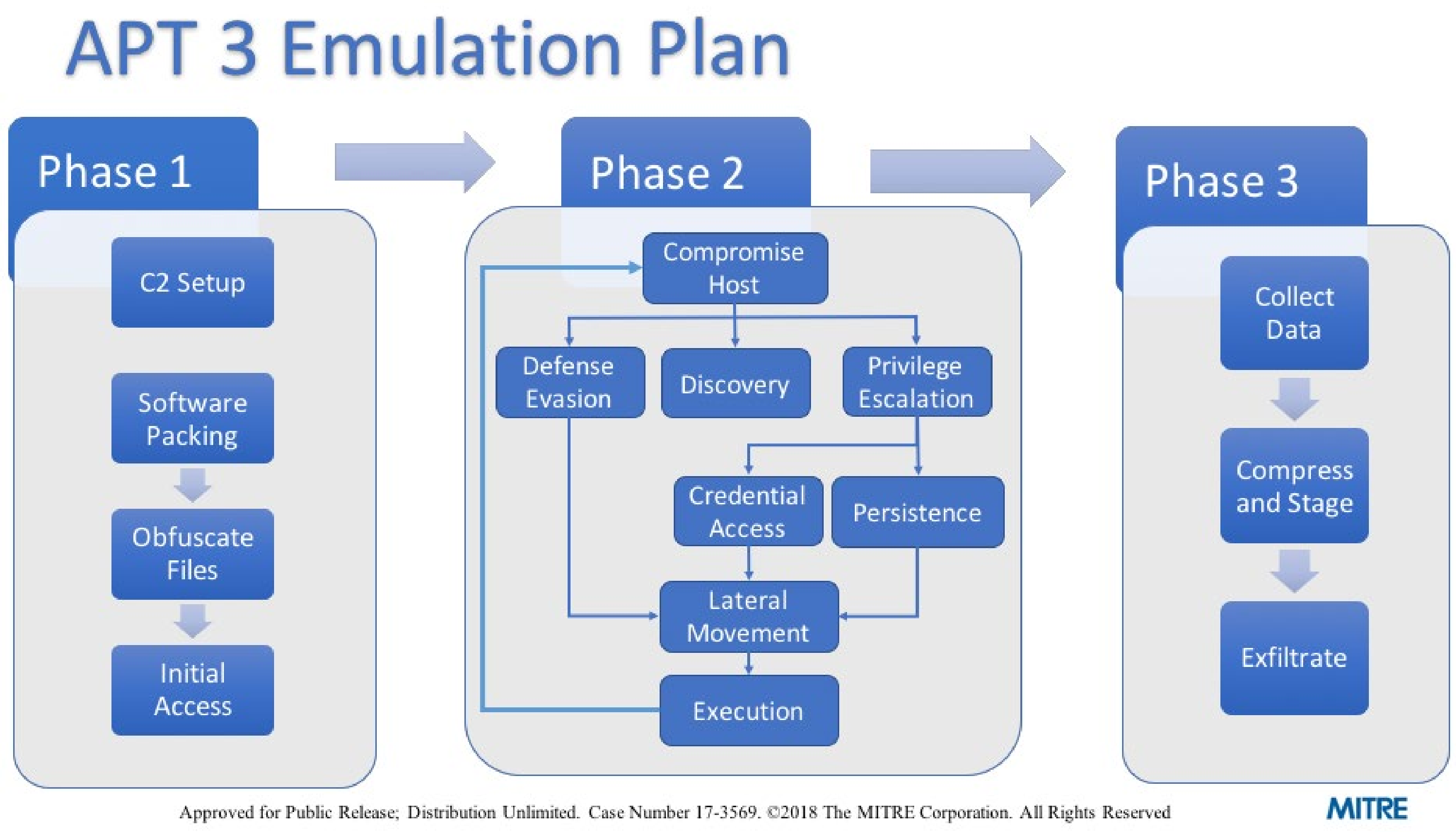
Technique

ID	T1189
Tactic	Initial Access
Platform	Linux, Windows, macOS
Permissions Required	User
Data Sources	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Contents [hide]

Source: https://attack.mitre.org/wiki/Main_Page

Mitre Adversarial Tactics, Techniques & Common Knowledge (ATTACK)



APT 3 Emulation Plan

Phase 1

- C2 Setup
- Software Packing
- Obfuscate Files
- Initial Access

Phase 2

- Compromise Host
- Defense Evasion
- Discovery
- Privilege Escalation
- Credential Access
- Persistence
- Lateral Movement
- Execution

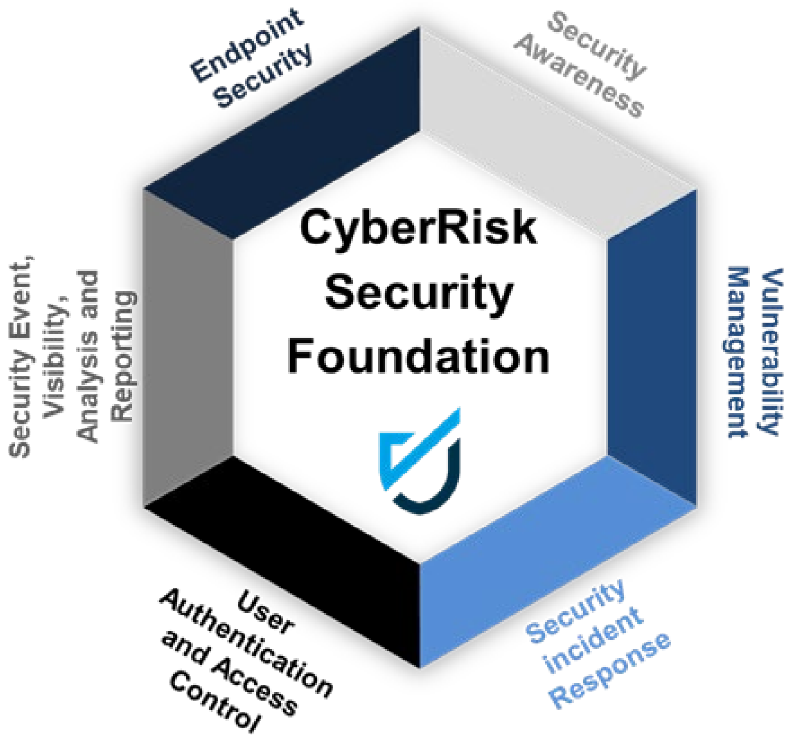
Phase 3

- Collect Data
- Compress and Stage
- Exfiltrate

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

MITRE

CyberRisk security foundation (minimum viable security)


CyberRisk Security Foundation
Endpoint Security
Security Awareness
Vulnerability Management
Security incident Response
User Authentication and Access Control
Security Event, Visibility, Analysis and Reporting

Putting it all together

Putting it all together

- Strategy, Planning and Design
    - Establish management support
    - Establish governance committee
    - **Asset identification and management**
    - Identify and classify sensitive data at rest and in transit
    - **Determine business drivers for security**
    - **Carry out a threat profile on the organisation**
    - **Carry out a risk assessment against Minimum Viable Security**
    - Develop security architecture
    - Identify solutions per architecture level
    - Establish goals and metrics

Putting it all together

- Implement
  - Develop and implement security policies, procedures, standards, baselines and guidelines
  - Assign roles and responsibilities
- Implement programs
  - Risk management
  - **Vulnerability and patch management**
  - Compliance
  - **Identity management and access control**
  - Change control
  - Software development life cycle
  - Business continuity planning
  - **Awareness and training**
  - Physical security
  - **Incident response**
  - **End point security**
  - **Auditing and monitoring**

Putting it all together

- Operate and Maintain
    - Operate, measure and run programs
    - Carry out internal and external audits and tests
- Monitor and evaluate
    - Review logs, audit results, collected metric values and SLAs per program
    - Assess goal accomplishments per program
    - Carry out quarterly meetings with governance committee
    - Develop improvement steps and integrate into the plan and organise phase
    - Assess and review risks

Putting it all together

- Minimum Viable Security
  - Asset awareness
  - Threat profiling
  - Security awareness
  - Vulnerability management and Patching
  - Control administrator rights
  - Endpoint security
  - Network visibility
  - Multifactor authentication
  - Incident response plan

Putting it all together

- Next week you should:
  - Assess yourself to determine your level of Minimum Viable Security
  - Identify your investments in each area. Are you under or over invested?
- In the first three months following this presentation you should:
  - Prepare plans to address any gaps
- Within six months you should:
  - Test your new or updated controls to confirm they work

Questions?

CyberRisk

PASSION • INTEGRITY • EXPERIENCE • RESULTS