Welcome

Security Lessons from Verizon's Analysis of 42,068 Security Incidents

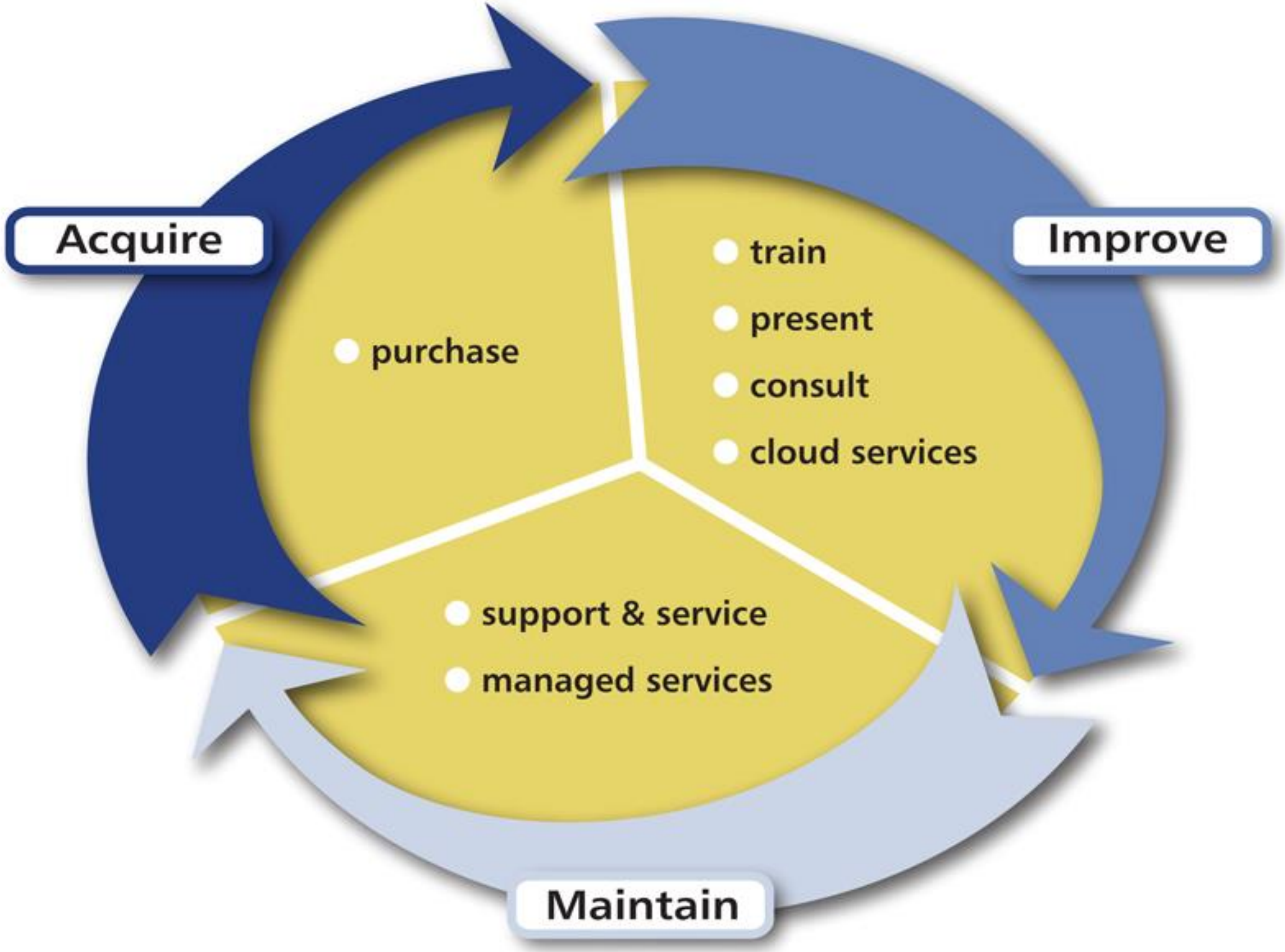
What do you hope to learn today?

Please take a moment to fill out the yellow cards.

Our presenters will review the cards to ensure we cover the topics/areas of interest.

We will collect them before we get started.

Thanks!



Acquire

- purchase

Improve

- train
- present
- consult
- cloud services

Maintain

- support & service
- managed services

Collect ‘Learn Today’ Cards

What do you hope to learn today?

Please take a moment to fill out the yellow cards.

Our presenters will review the cards to ensure we cover the topics/areas of interest.

We will collect them before we get started

Thanks!

Our Management Seminar Series

- ✓ Security Lessons from Verizon's Analysis of 42,068 Security Incidents
- Learning from our 145,000 Completed IT Support Tickets and 13,750 Satisfaction Surveys
- Reducing Your IT Costs
- Evaluating Managed IT Services
- Cloud Strategy
- DR Planning
- Building a Cost Effective and Crisis Free IT Team

Agenda

- Your security agenda
- Report basics
- Breach trends
- Incident classification patterns
- Gartner’s insource/outsource recommendation
- Possible actions

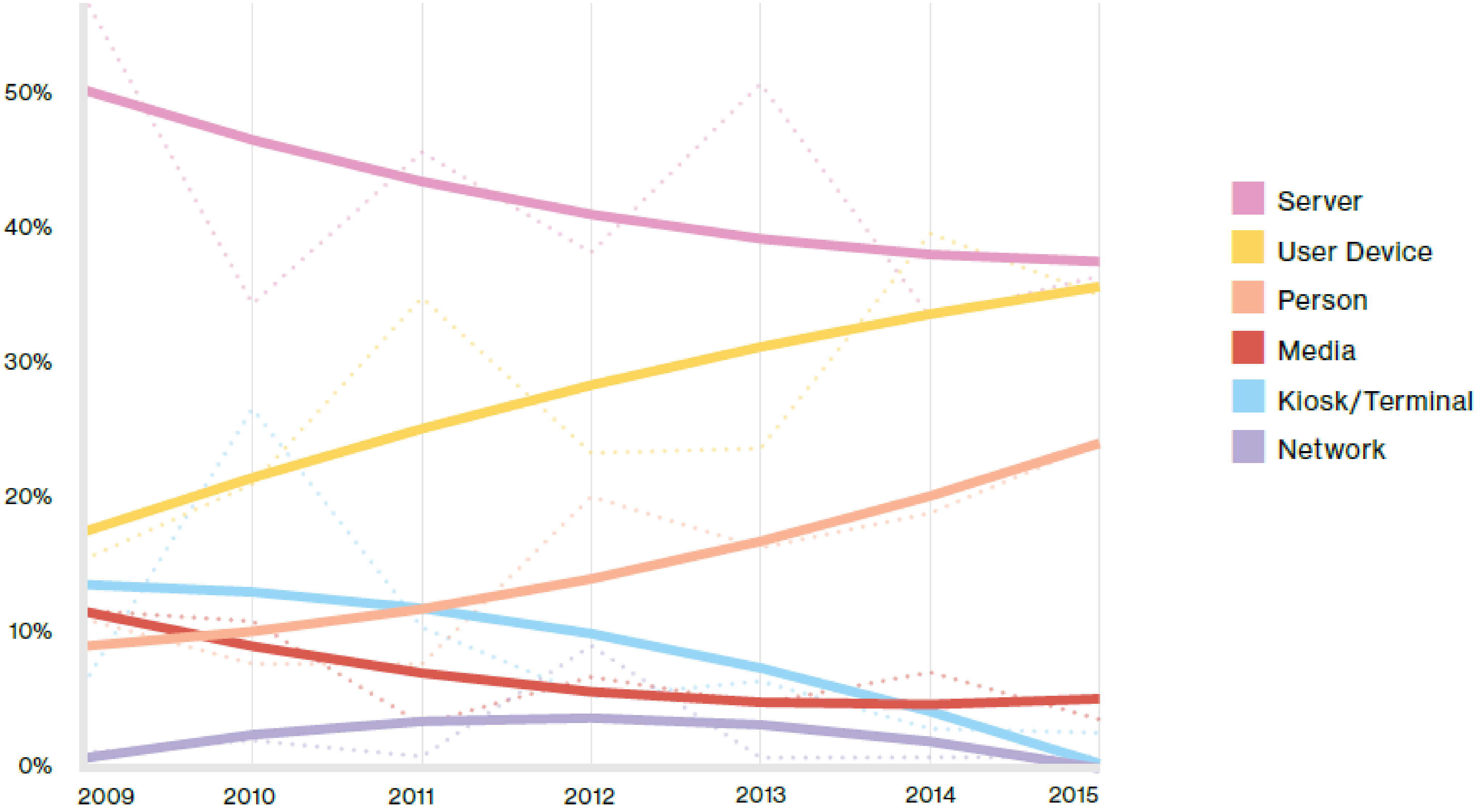
Verizon Data Breach Investigations Report

- 62 organizations contribute world-wide
  - From Akamai to Homeland Security
- Lists threats, vulnerabilities and actions leading to security incidents and data breaches
- Categorized by industry using NAICS codes
- 10th year

Secondary Attacks Prevalent

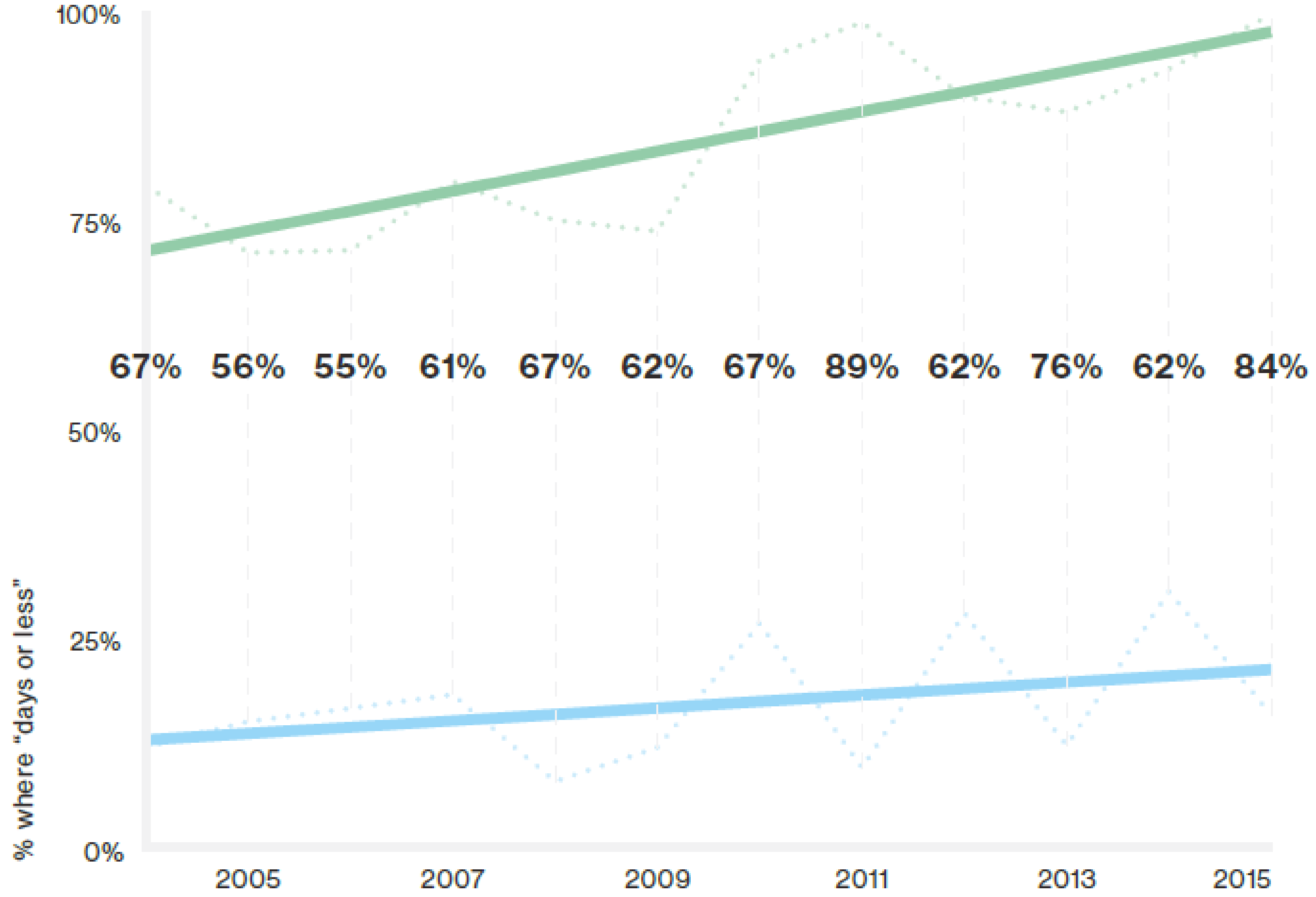
- 70% of attacks with known motives involve a secondary victim
- Servers compromised for denial-of service (DoS) attacks, hosting malware or for phishing site

Percentage of Breaches per Asset Category



Breach Discovery “Detection Deficit”

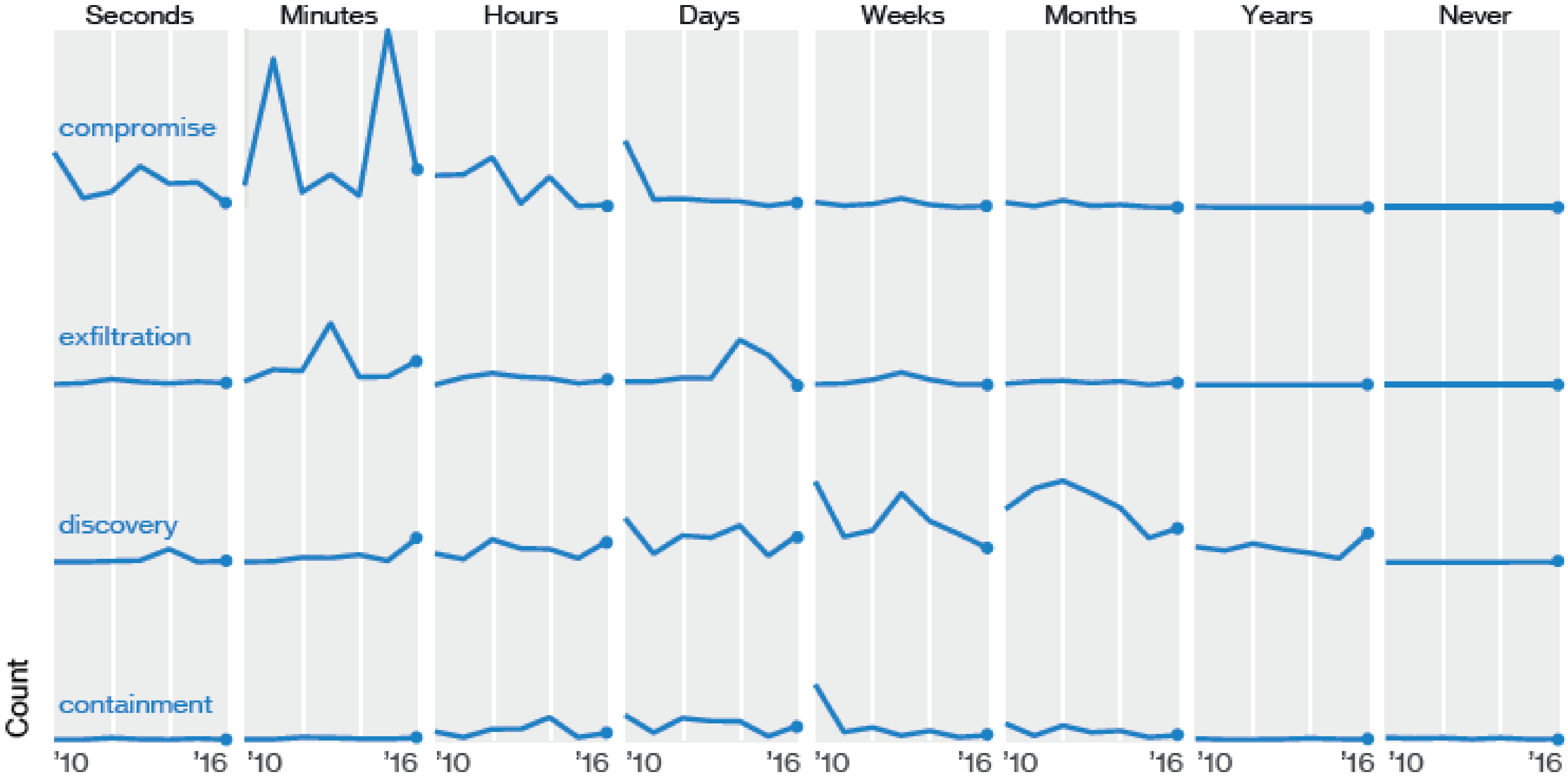
compares how often attackers compromised a victim in days or less (green) with how often defenders detected compromises in same time frame (blue).



60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

Timespan of breach events over time

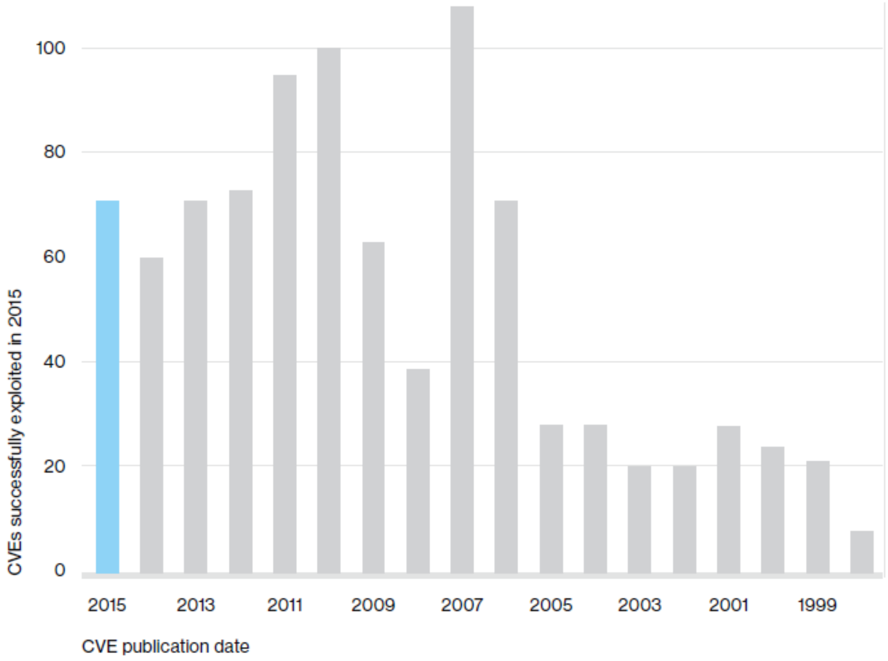


Sharing Threat Information

- How fast intelligence needs to be shared
  - 75% of attacks spread from Victim 0 to Victim 1 within 24 hours - 40% < hour
  - Most IP addresses on the block/alert list < 1 day
- Breadth of intelligence to be shared
  - Phishing infrastructure is 9K domains and 50K URLs monthly

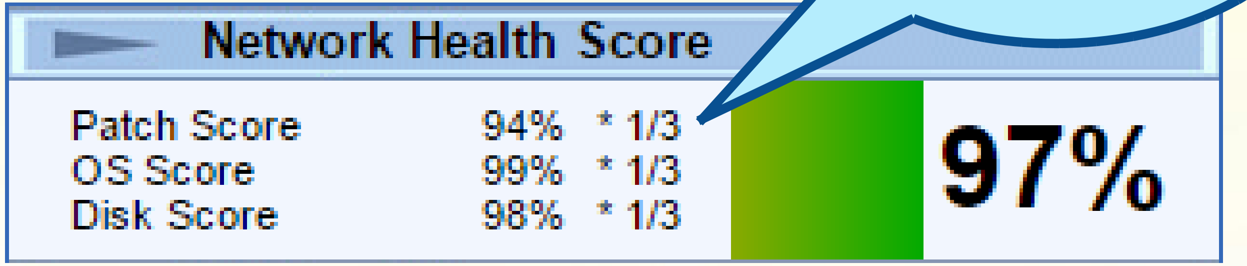
Vulnerabilities

- Vast majority of exploited vulnerabilities compromised > year after publication
- Patch broadly and consistently - more effective than urgently patching at release



Action - Performance Reporting

35% score before onboarding
Increases to 94% with attention



Network Health Score

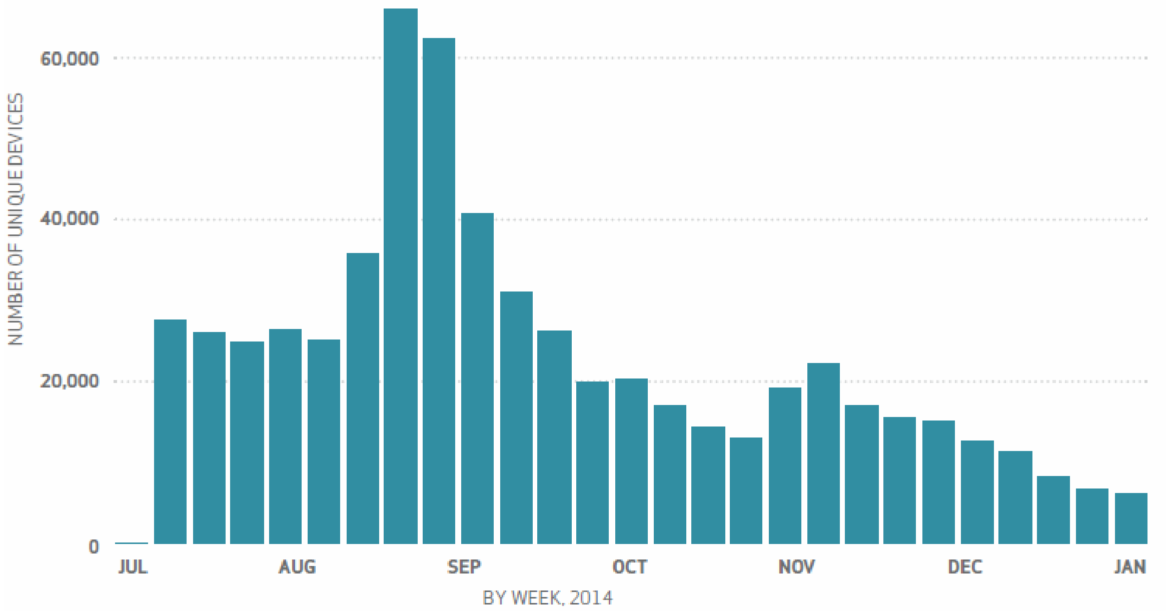
Patch Score	94%	* 1/3
OS Score	99%	* 1/3
Disk Score	98%	* 1/3

97%

Mobile

- Android wins at malicious activity (96%)
  - iOS activity mainly failed Android exploits!
  - Mainly annoyance and resource wasting infections
- Mobile not preferred path to breaches

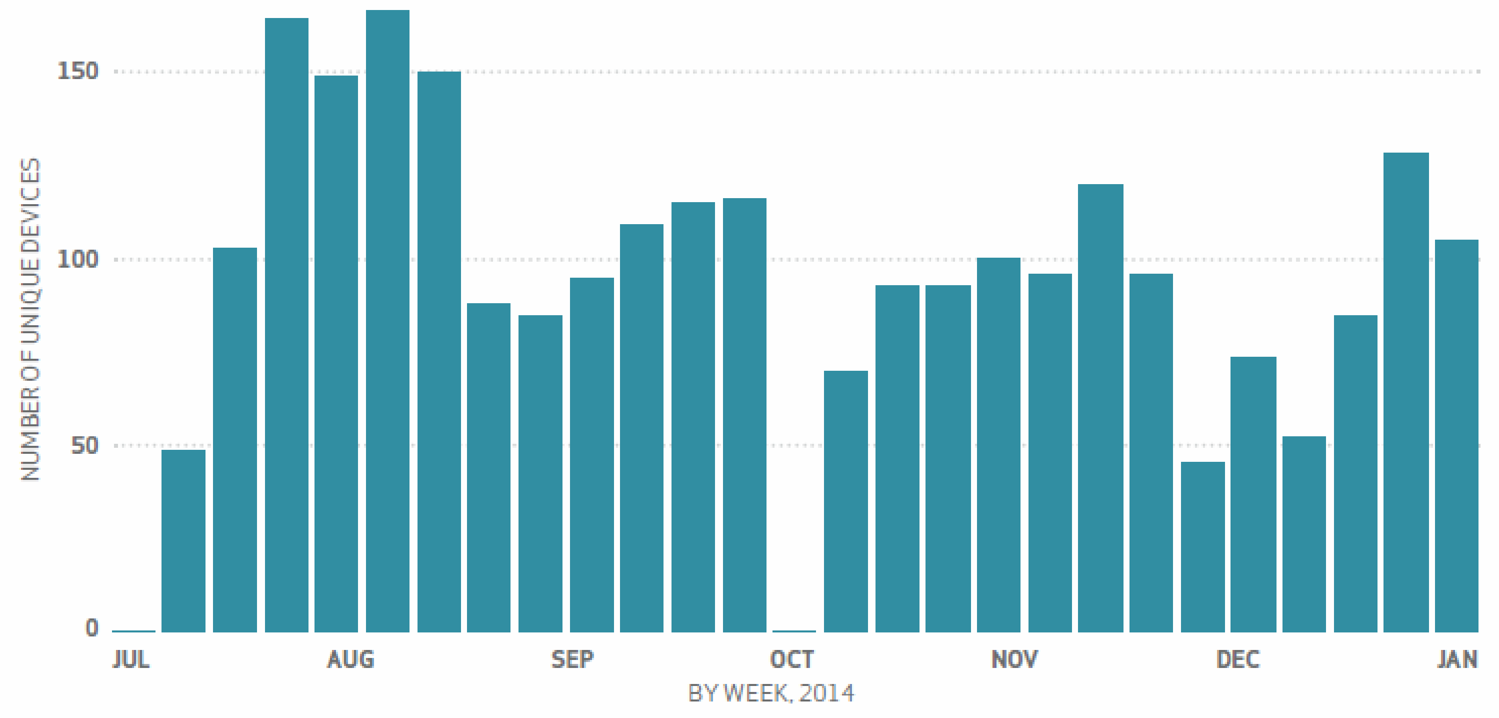
Count of all detected mobile malware infections



Mobile

- VZ Wireless supplied data stripped of low grade malware and adnoyance found count of compromised devices negligible – 0.03% per week

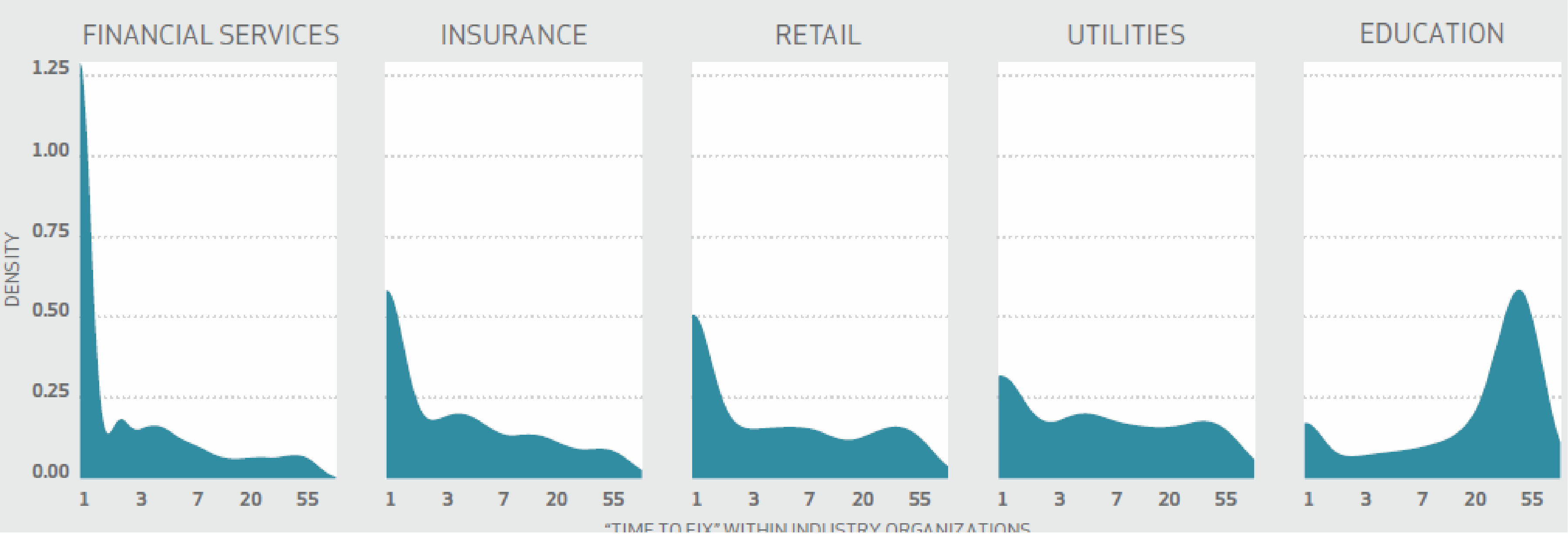
Count of all non-adnoyance mobile malware infections



Malware

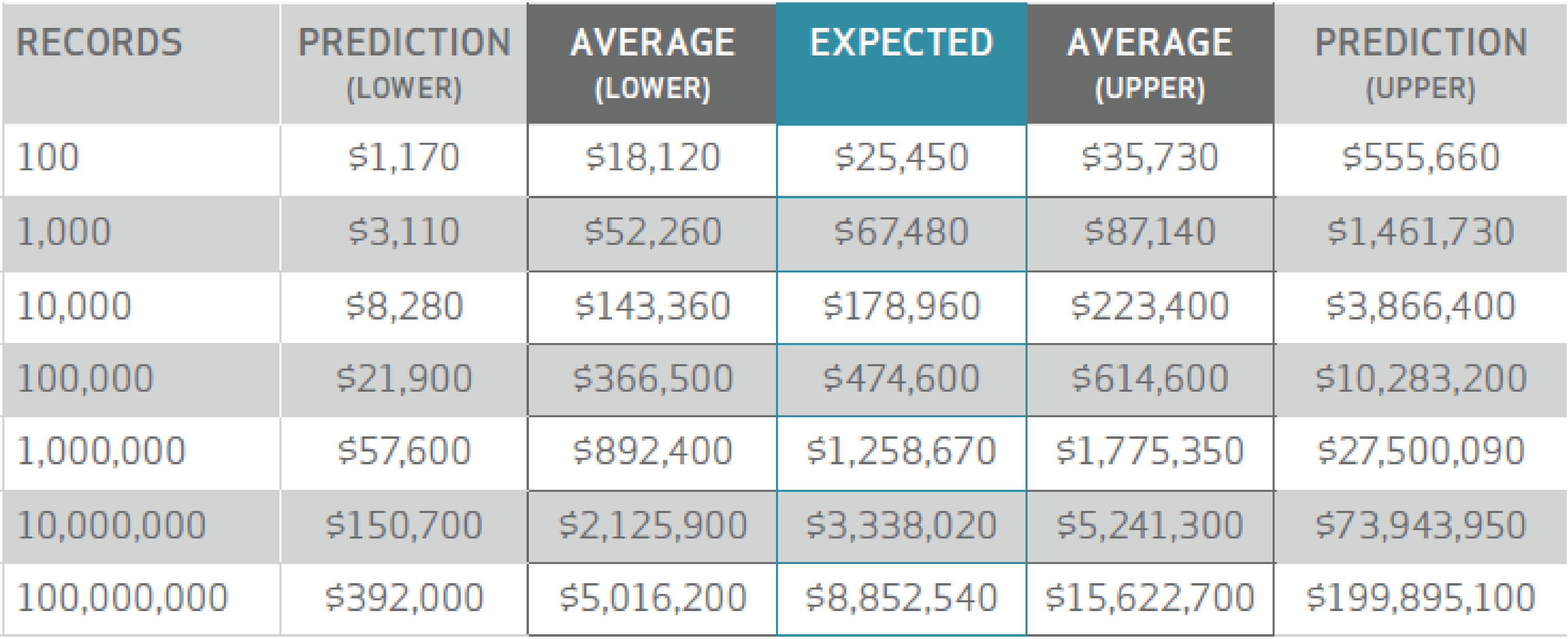
- Data by industry shows financial services, insurance, retail, utilities and education are leading risk sectors with varying signatures

Distribution of “time to fix” by industry vertical



Impact

Linear cost/record moves to more statistically sound $ ranges

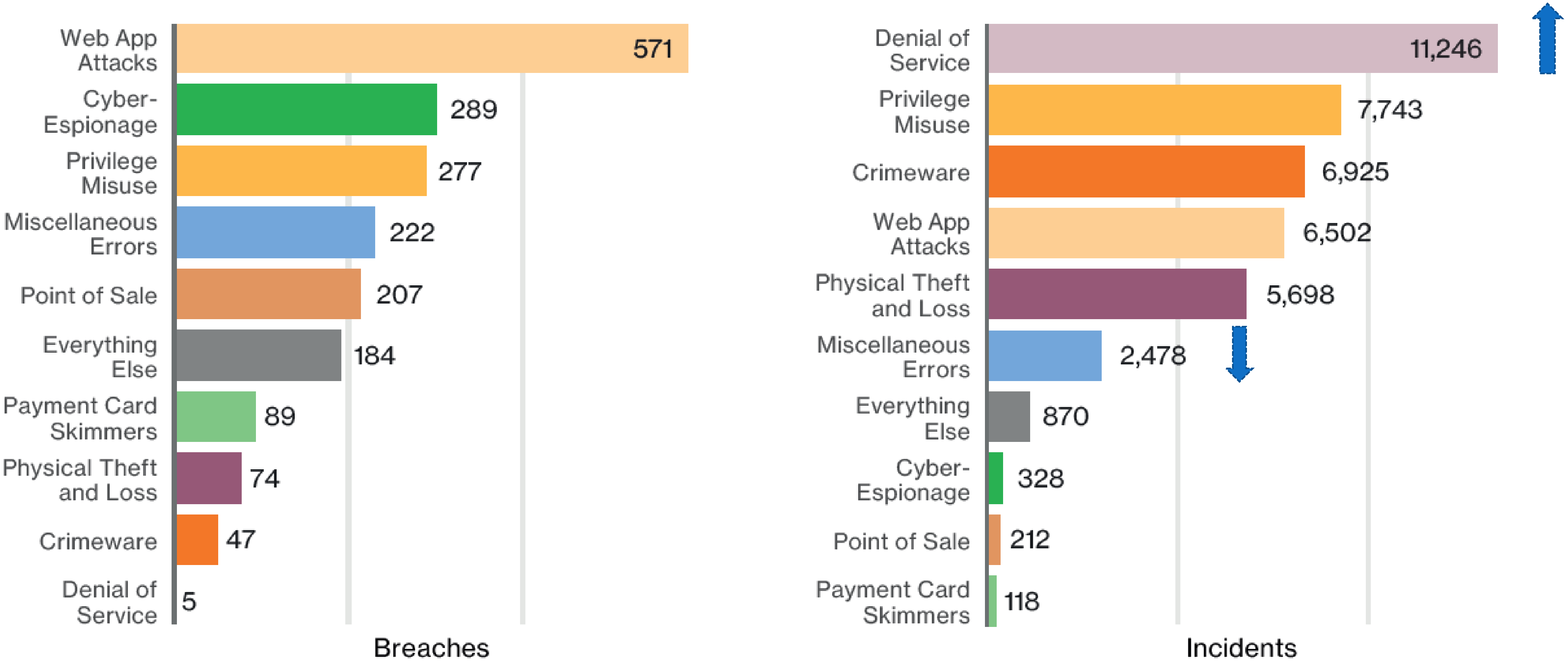


RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Ranges of expected loss by # of records

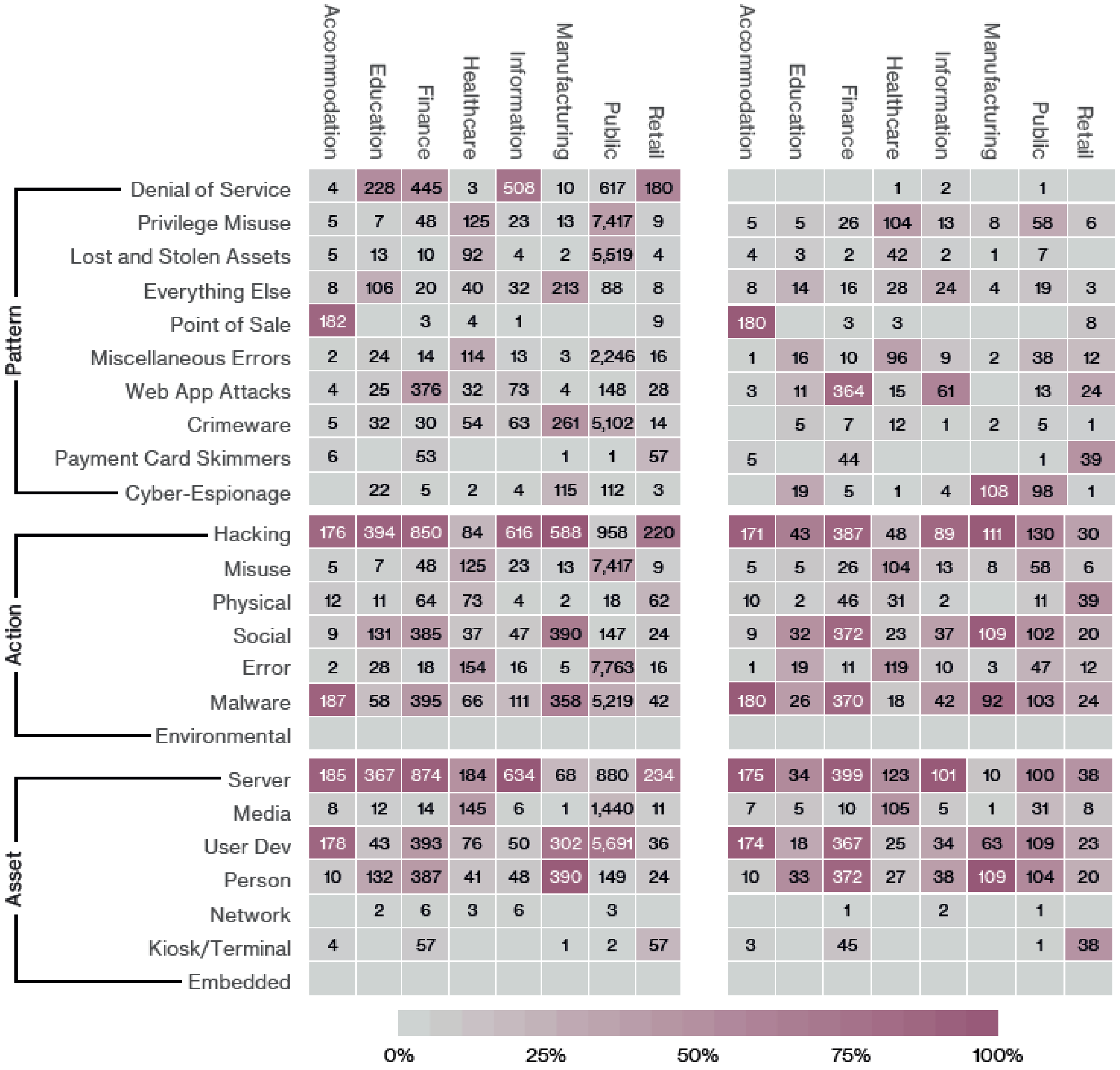
Incident Classification Patterns

88% of 42K incidents covered by top 9 patterns



Frequency of incident patterns across “security incidents” (right) and “data breaches” (left)

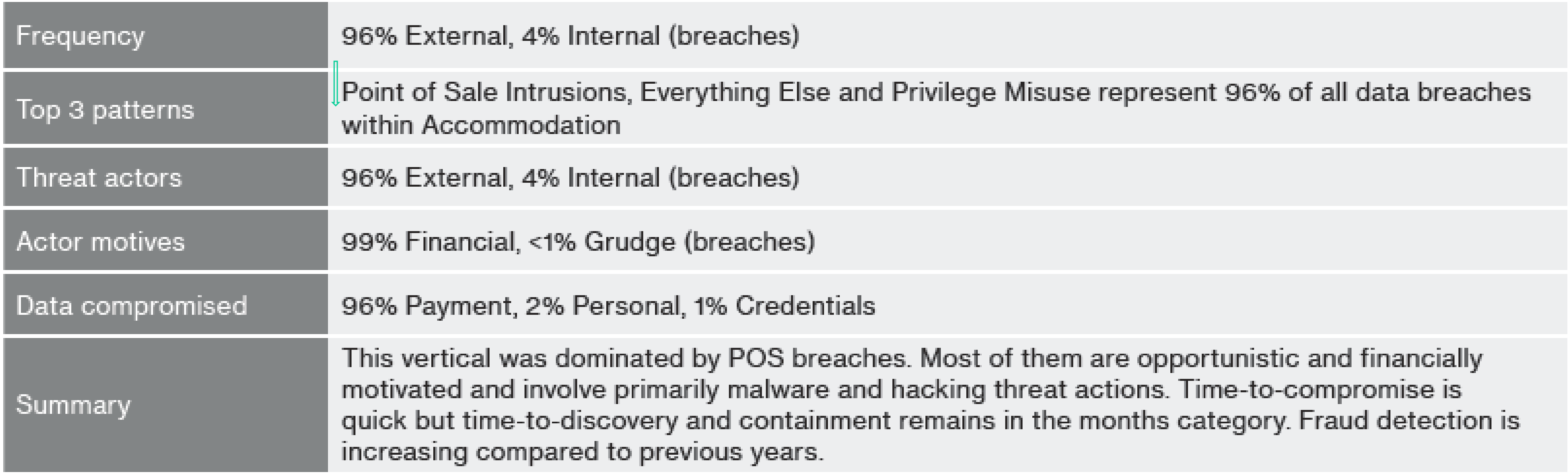
Industry Comparison



		Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail	Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
Pattern	Denial of Service	4	228	445	3	508	10	617	180				1	2		1	
	Privilege Misuse	5	7	48	125	23	13	7,417	9	5	5	26	104	13	8	58	6
	Lost and Stolen Assets	5	13	10	92	4	2	5,519	4	4	3	2	42	2	1	7	
	Everything Else	8	106	20	40	32	213	88	8	8	14	16	28	24	4	19	3
	Point of Sale	182		3	4	1			9	180		3	3				8
	Miscellaneous Errors	2	24	14	114	13	3	2,246	16	1	16	10	96	9	2	38	12
	Web App Attacks	4	25	376	32	73	4	148	28	3	11	364	15	61		13	24
	Crimeware	5	32	30	54	63	261	5,102	14		5	7	12	1	2	5	1
	Payment Card Skimmers	6		53			1	1	57	5		44				1	39
	Cyber-Espionage		22	5	2	4	115	112	3		19	5	1	4	108	98	1
Action	Hacking	176	394	850	84	616	588	958	220	171	43	387	48	89	111	130	30
	Misuse	5	7	48	125	23	13	7,417	9	5	5	26	104	13	8	58	6
	Physical	12	11	64	73	4	2	18	62	10	2	46	31	2		11	39
	Social	9	131	385	37	47	390	147	24	9	32	372	23	37	109	102	20
	Error	2	28	18	154	16	5	7,763	16	1	19	11	119	10	3	47	12
	Malware	187	58	395	66	111	358	5,219	42	180	26	370	18	42	92	103	24
	Environmental																
Asset	Server	185	367	874	184	634	68	880	234	175	34	399	123	101	10	100	38
	Media	8	12	14	145	6	1	1,440	11	7	5	10	105	5	1	31	8
	User Dev	178	43	393	76	50	302	5,691	36	174	18	367	25	34	63	109	23
	Person	10	132	387	41	48	390	149	24	10	33	372	27	38	109	104	20
	Network		2	6	3	6		3				1		2		1	
	Kiosk/Terminal	4		57			1	2	57	3		45				1	38
	Embedded																

Figure 9: Industry comparison (left: all security incidents, right: breaches only)

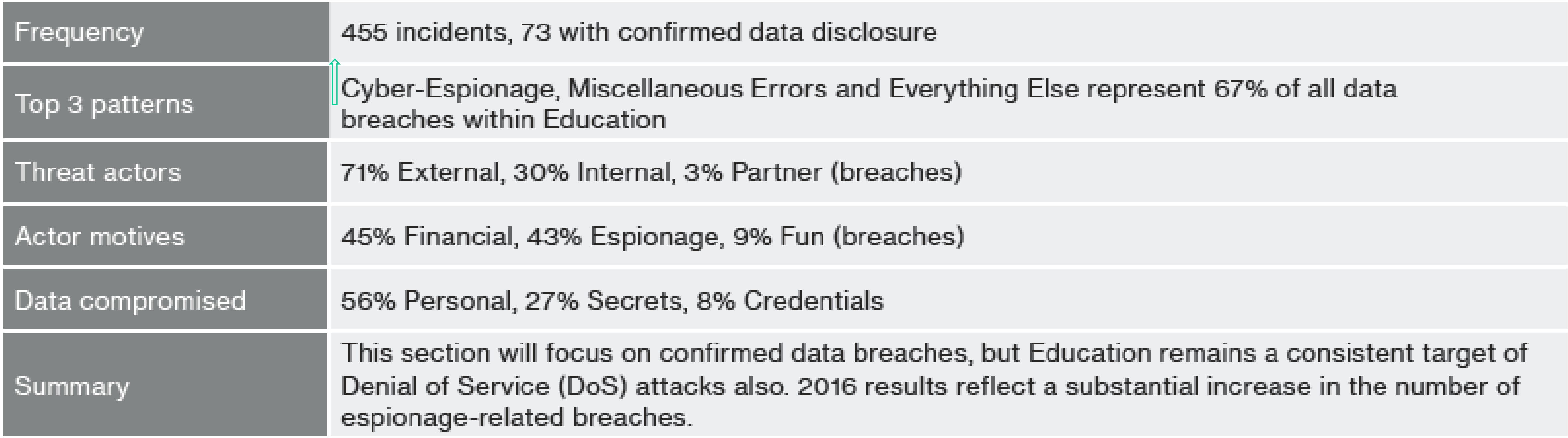
Accommodation and Food Services



Frequency	96% External, 4% Internal (breaches)
Top 3 patterns	Point of Sale Intrusions, Everything Else and Privilege Misuse represent 96% of all data breaches within Accommodation
Threat actors	96% External, 4% Internal (breaches)
Actor motives	99% Financial, <1% Grudge (breaches)
Data compromised	96% Payment, 2% Personal, 1% Credentials
Summary	This vertical was dominated by POS breaches. Most of them are opportunistic and financially motivated and involve primarily malware and hacking threat actions. Time-to-compromise is quick but time-to-discovery and containment remains in the months category. Fraud detection is increasing compared to previous years.

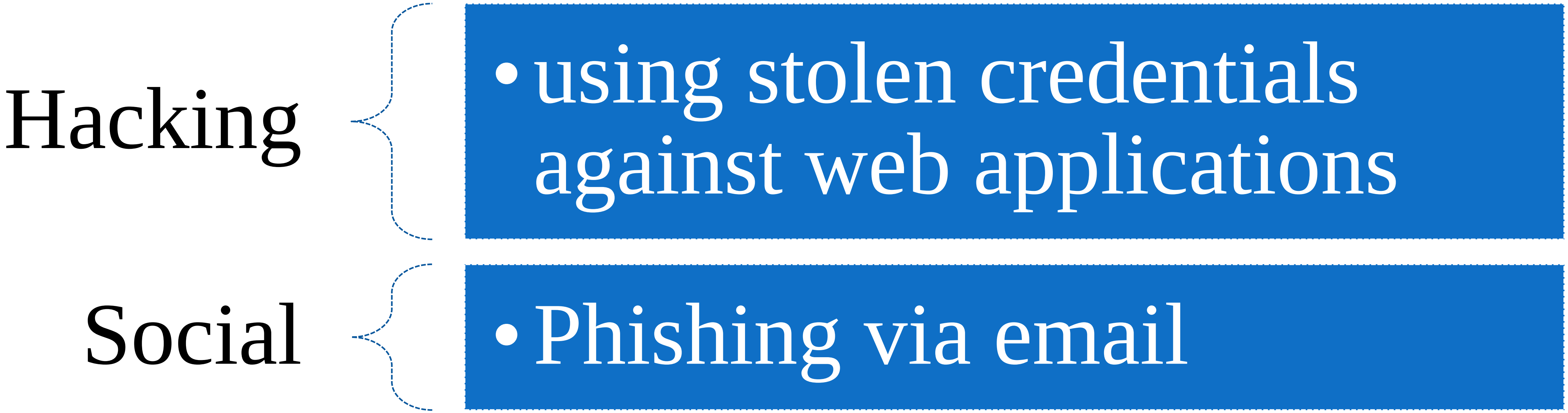
Decrease malware installation (94% of breaches)
No default passwords
Only allow connections from whitelisted IPs to POS network
Patch promptly and consistently

Educational Services



Frequency	455 incidents, 73 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Miscellaneous Errors and Everything Else represent 67% of all data breaches within Education
Threat actors	71% External, 30% Internal, 3% Partner (breaches)
Actor motives	45% Financial, 43% Espionage, 9% Fun (breaches)
Data compromised	56% Personal, 27% Secrets, 8% Credentials
Summary	This section will focus on confirmed data breaches, but Education remains a consistent target of Denial of Service (DoS) attacks also. 2016 results reflect a substantial increase in the number of espionage-related breaches.

Educational Services Threat Categories



Hacking

- using stolen credentials against web applications

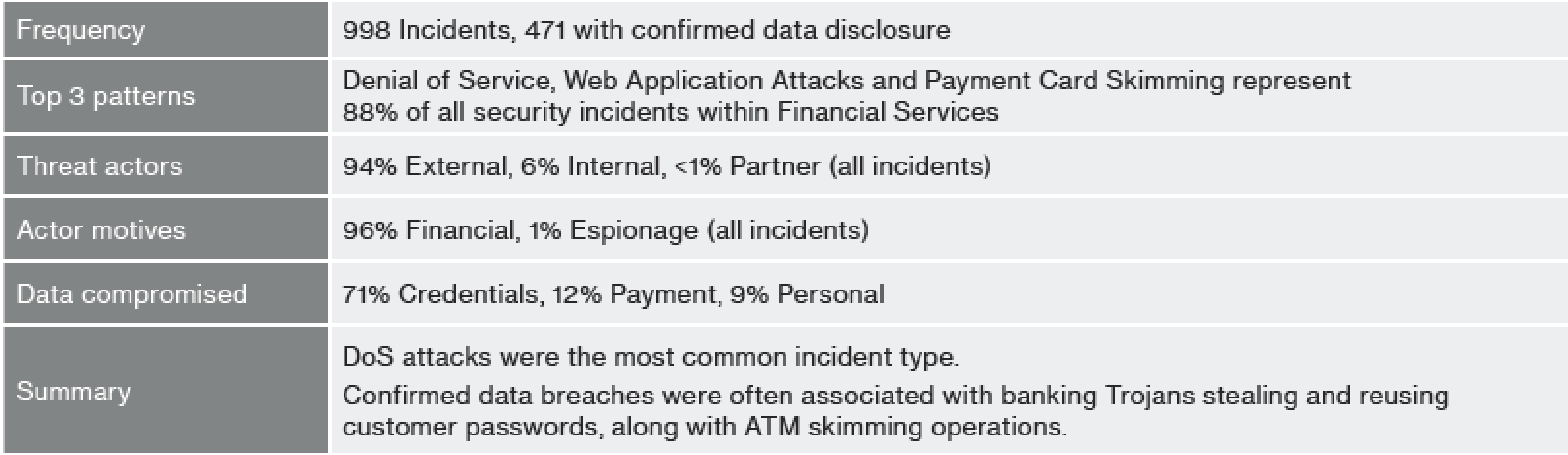
Social

- Phishing via email

Educational Services Top Actions

- Train employees and students on security awareness and encourage reporting of suspicious activity such as phishing or pretexting attacks
- Develop response plan and practice disaster and recovery plans to prepare for unreasonably high traffic

Financial and Insurance



Frequency	998 Incidents, 471 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Payment Card Skimming represent 88% of all security incidents within Financial Services
Threat actors	94% External, 6% Internal, <1% Partner (all incidents)
Actor motives	96% Financial, 1% Espionage (all incidents)
Data compromised	71% Credentials, 12% Payment, 9% Personal
Summary	DoS attacks were the most common incident type. Confirmed data breaches were often associated with banking Trojans stealing and reusing customer passwords, along with ATM skimming operations.

Financial and Insurance Threat Categories

(After removing ATM skimming, DoS, and botnets)

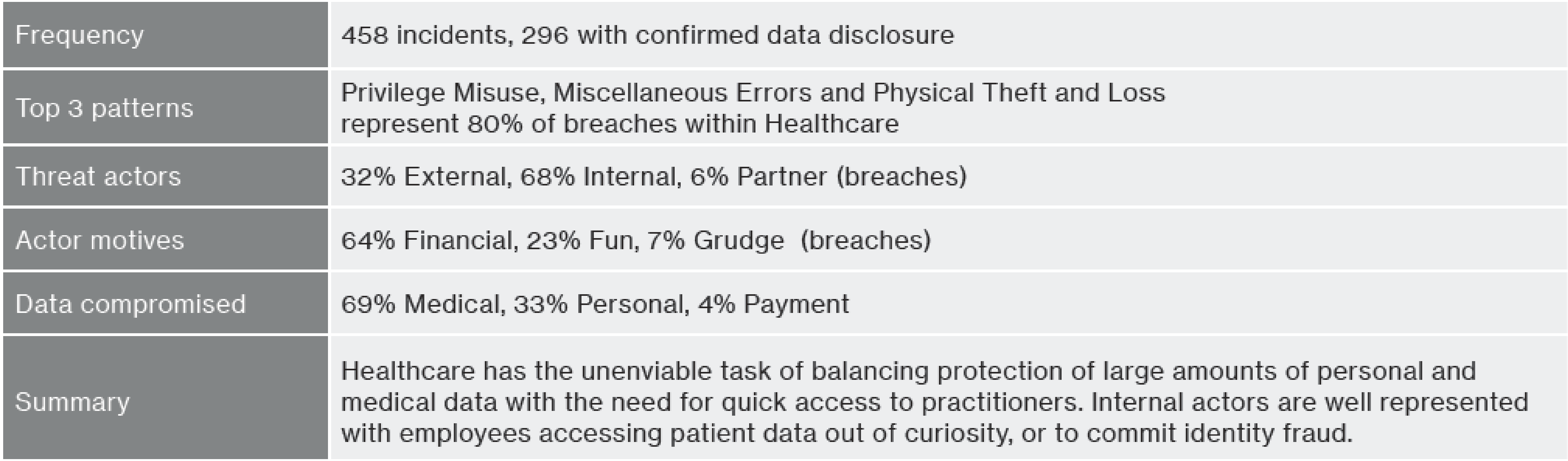
Privilege Misuse

- Accessing systems to fraudulently transfer money
- Using customer information for identity theft

Financial and Insurance Top Actions

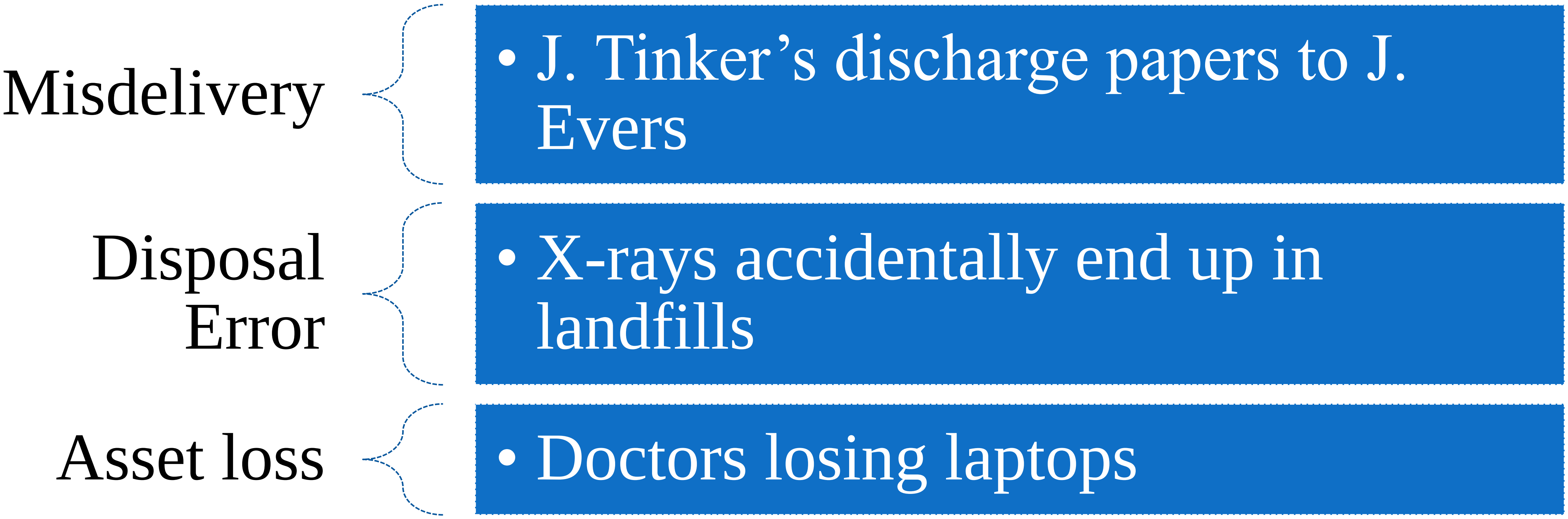
- Train users on security awareness and encourage reporting of suspicious activity
- Have a DoS mitigation service and know the service scope
- Periodically monitor employee activities. Give permissions only if needed and disable accounts immediately at exit.

Healthcare



Frequency	458 incidents, 296 with confirmed data disclosure
Top 3 patterns	Privilege Misuse, Miscellaneous Errors and Physical Theft and Loss represent 80% of breaches within Healthcare
Threat actors	32% External, 68% Internal, 6% Partner (breaches)
Actor motives	64% Financial, 23% Fun, 7% Grudge (breaches)
Data compromised	69% Medical, 33% Personal, 4% Payment
Summary	Healthcare has the unenviable task of balancing protection of large amounts of personal and medical data with the need for quick access to practitioners. Internal actors are well represented with employees accessing patient data out of curiosity, or to commit identity fraud.

Top Healthcare Threat Categories (80%)



Misdelivery

- J. Tinker's discharge papers to J. Evers

Disposal Error

- X-rays accidentally end up in landfills

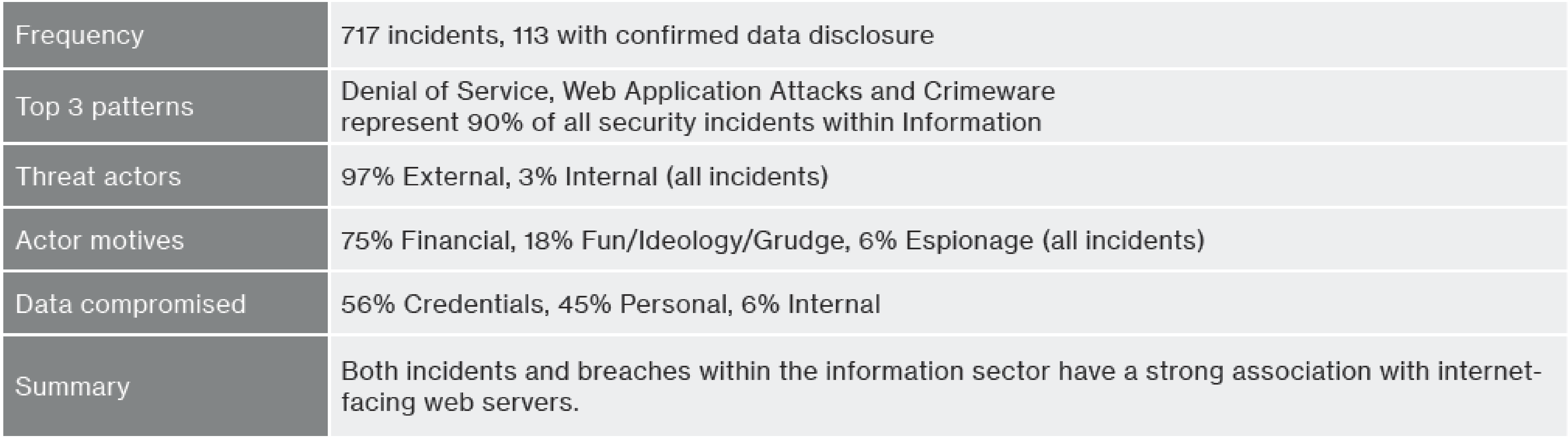
Asset loss

- Doctors losing laptops

Healthcare Top Actions

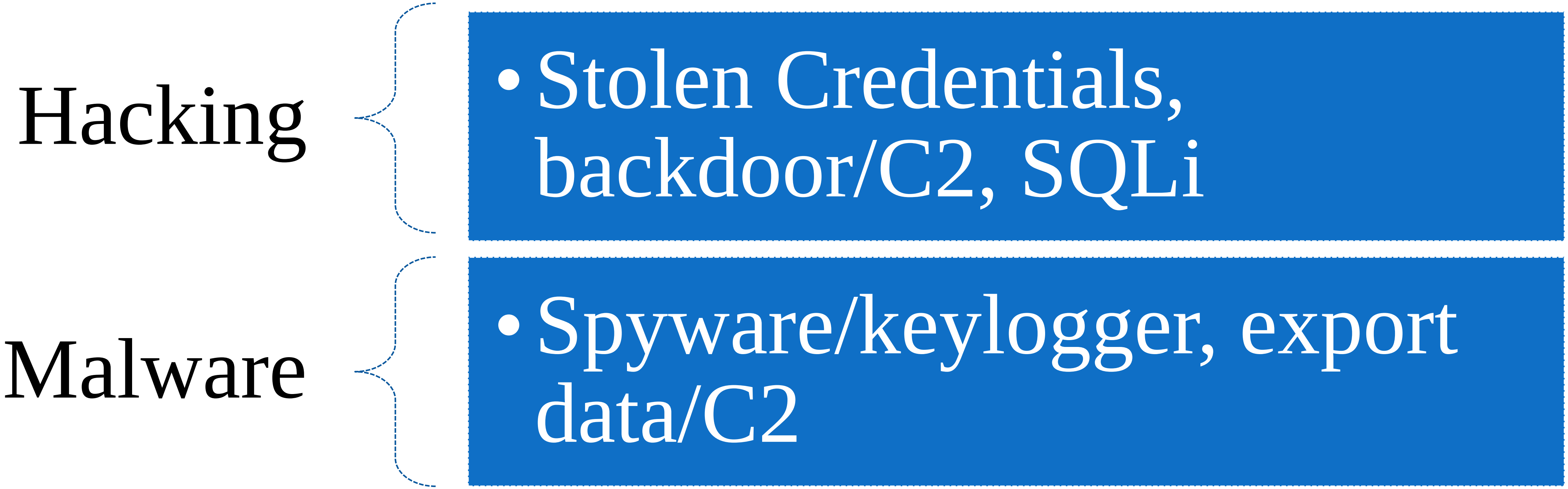
- Process to prevent errors (*Checklist Manifesto*)
- Disposal policy for PII including monitoring
- Encrypt mobile devices to limit impact of lost assets

Information



Frequency	717 incidents, 113 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Crimeware represent 90% of all security incidents within Information
Threat actors	97% External, 3% Internal (all incidents)
Actor motives	75% Financial, 18% Fun/Ideology/Grudge, 6% Espionage (all incidents)
Data compromised	56% Credentials, 45% Personal, 6% Internal
Summary	Both incidents and breaches within the information sector have a strong association with internet-facing web servers.

Top Information Threat Categories



Hacking

- Stolen Credentials, backdoor/C2, SQLi

Malware

- Spyware/keylogger, export data/C2

Information Top Actions

- Implement 2FA for admin access to web apps and data stores
- Extend strong authentication to app users
- Develop DDoS response plan within BC and DR plans
- Patch server software (OS, web applications, plug-ins)

Manufacturing

Frequency	620 incidents, 124 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Everything Else represent 96% of breaches within Manufacturing
Threat actors	93% External , 7% Internal (breaches)
Actor motives	94% Espionage, 6% Financial (breaches)
Data compromised	91% Secrets, 4% Internal, 4% Personal
Summary	Gains in strategic advantage via espionage-related actions comprise the majority of breaches within this industry. Most are conducted by state-affiliated actors, but instances of internal espionage pilfering trade secrets are present as well.

Top Manufacturing Threat Categories

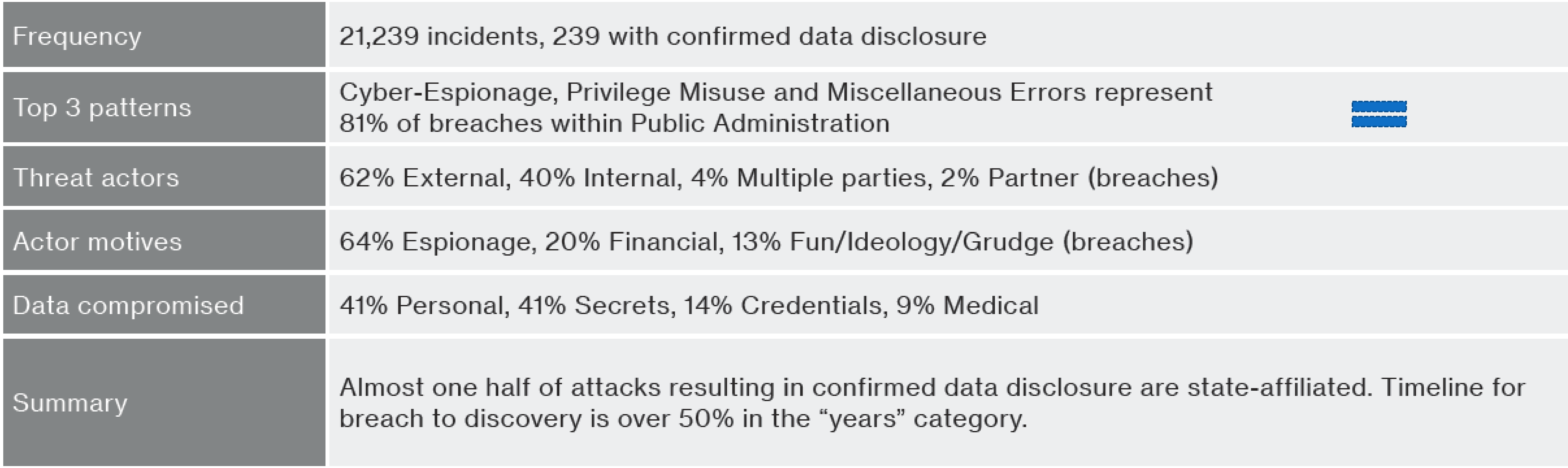
Cyber-Espionage

- Stealing IP for competitive advantage

Manufacturing Top Actions

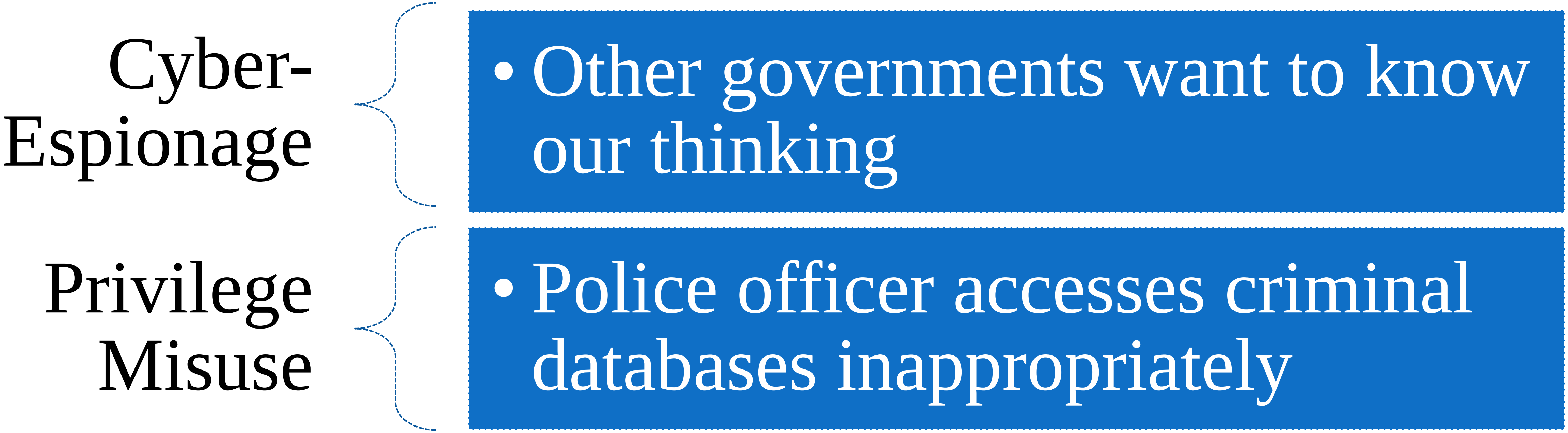
- Sensitive data is separated with need to know access
- Train employees against phishing and easy ways to report suspicious emails
- Monitor internal network, devices and applications
  - Accounts monitoring
  - Audit log monitoring
  - IDS monitoring
- DLP

Public Administration



Frequency	21,239 incidents, 239 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Miscellaneous Errors represent 81% of breaches within Public Administration
Threat actors	62% External, 40% Internal, 4% Multiple parties, 2% Partner (breaches)
Actor motives	64% Espionage, 20% Financial, 13% Fun/Ideology/Grudge (breaches)
Data compromised	41% Personal, 41% Secrets, 14% Credentials, 9% Medical
Summary	Almost one half of attacks resulting in confirmed data disclosure are state-affiliated. Timeline for breach to discovery is over 50% in the "years" category.

Top Public Administration Threat Categories



Cyber-Espionage

- Other governments want to know our thinking

Privilege Misuse

- Police officer accesses criminal databases inappropriately

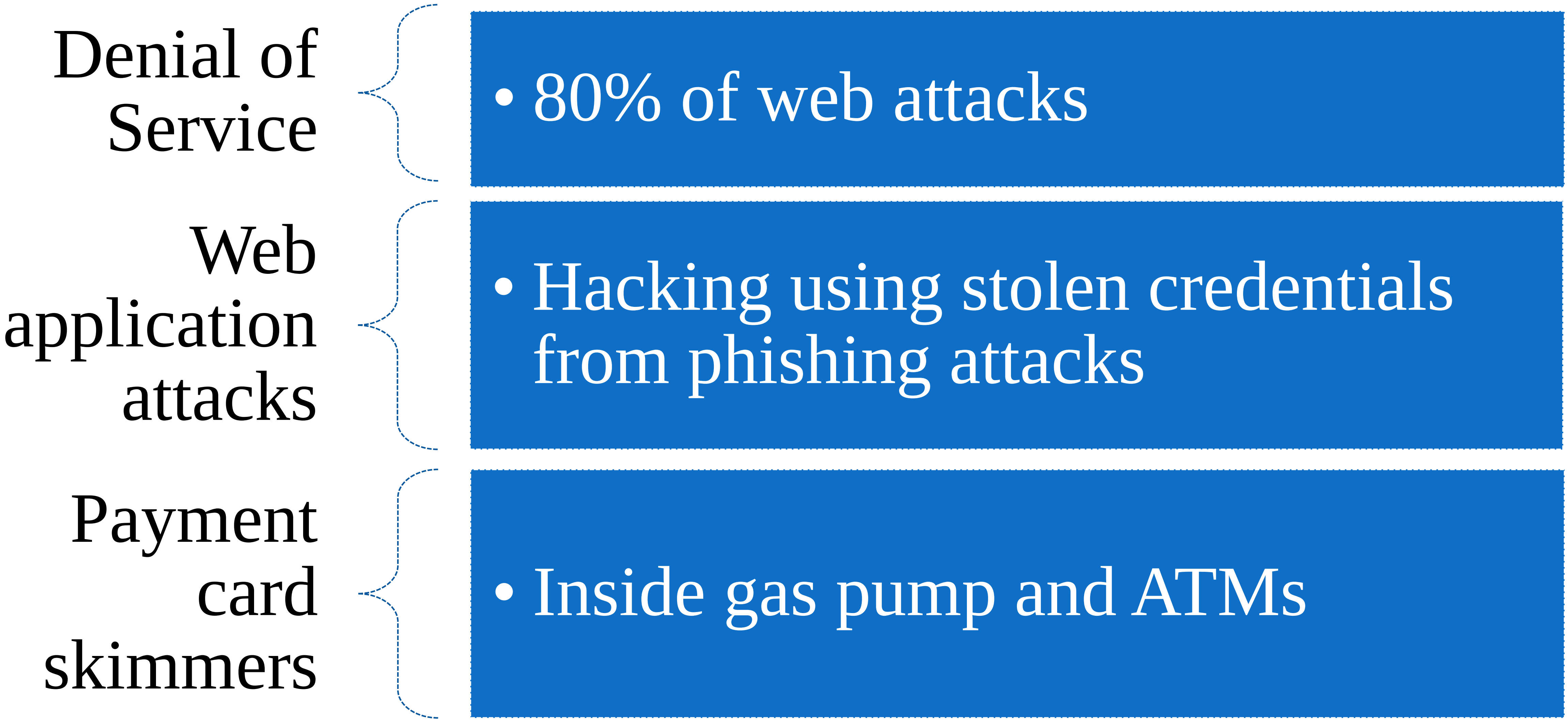
Public Administration Top Actions

- Know sensitive data, where it resides, who has access rights and who does access
- DLP and data egress logging
- Understand type of threat actor most interested in your data

Retail

Frequency	326 incidents, 93 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Payment Card Skimming represent 81% of all security incidents within Retail
Threat actors	92% External, 7% Internal, <1% Partner (incidents)
Actor motives	96% Financial, 2% Espionage, 2% Curiosity (incidents)
Data compromised	57% Payment, 27% Personal, 17% Credentials
Summary	Online retailers are consistent targets of DoS attacks, and POS environments continue to be compromised for financial motivations.

Top Retail Threat Categories



Denial of Service

- 80% of web attacks

Web application attacks

- Hacking using stolen credentials from phishing attacks

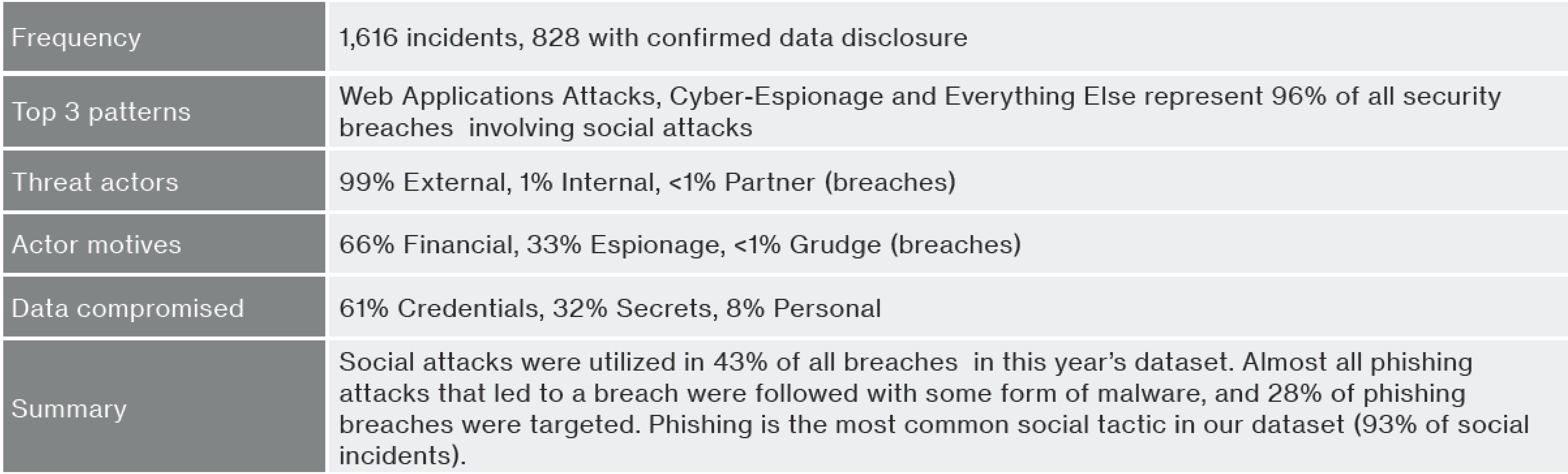
Payment card skimmers

- Inside gas pump and ATMs

Retail Top Actions

- Denial of service mitigation plans
- Keep critical assets on a separate network
- Implement strong passwords with 2FA especially for remote access into payment processing networks

Social Attacks



Frequency	1,616 incidents, 828 with confirmed data disclosure
Top 3 patterns	Web Applications Attacks, Cyber-Espionage and Everything Else represent 96% of all security breaches involving social attacks
Threat actors	99% External, 1% Internal, <1% Partner (breaches)
Actor motives	66% Financial, 33% Espionage, <1% Grudge (breaches)
Data compromised	61% Credentials, 32% Secrets, 8% Personal
Summary	Social attacks were utilized in 43% of all breaches in this year’s dataset. Almost all phishing attacks that led to a breach were followed with some form of malware, and 28% of phishing breaches were targeted. Phishing is the most common social tactic in our dataset (93% of social incidents).

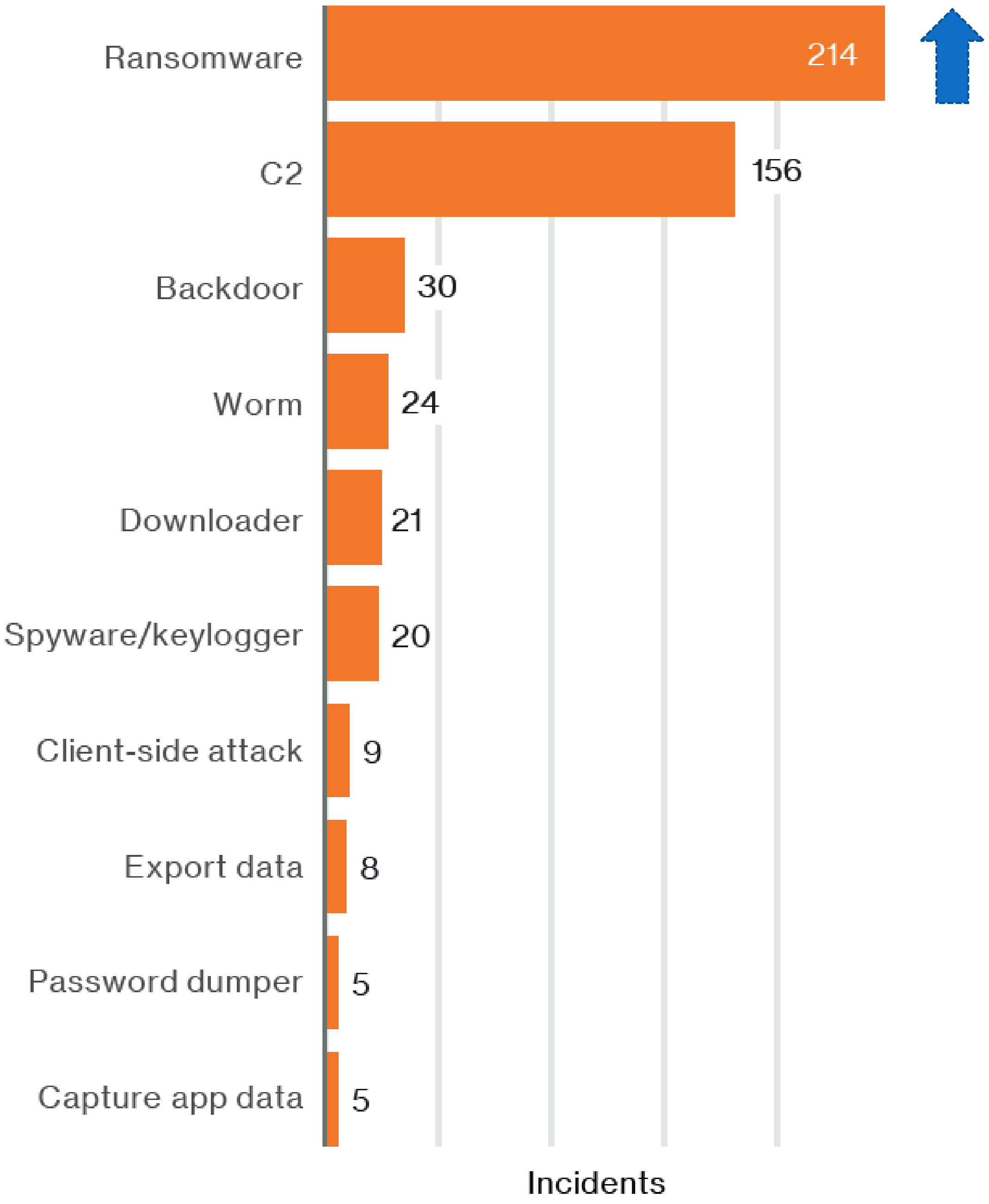
Phishing

- 30% opened phishing email - 12% of total click attachment - 7.3% of users were successfully phished
- 15% of those who fell victim twice - 3% clicked > twice - <1% clicked > three times
- Many sent as steady campaign – just 10 e-mails yield > 90% chance one person opens attachment
- Median time to click attachment = 3.7 min

Crimeware

= malware not associated with patterns like cyber espionage or POS intrusions

Variety of malware within Crimeware pattern



Ransomware

- Ransomware attacks not counted as breaches because typically data loss cannot be confirmed.
  - HHS given guidance that ransomware should be reported as a breach – now 72% of malware incidents in Healthcare
- From 22nd → 5th most common malware in 2014
- Social actions, notably phishing moving from 8% → 21% of incidents in 2016
  - Emails often targeted at job functions - HR and accounting

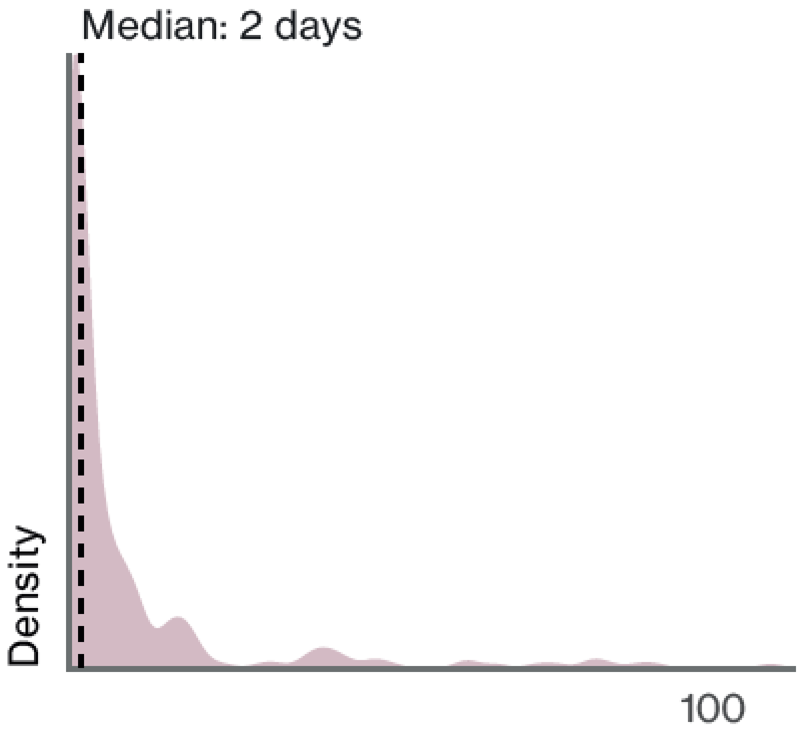
Crimeware Top Actions

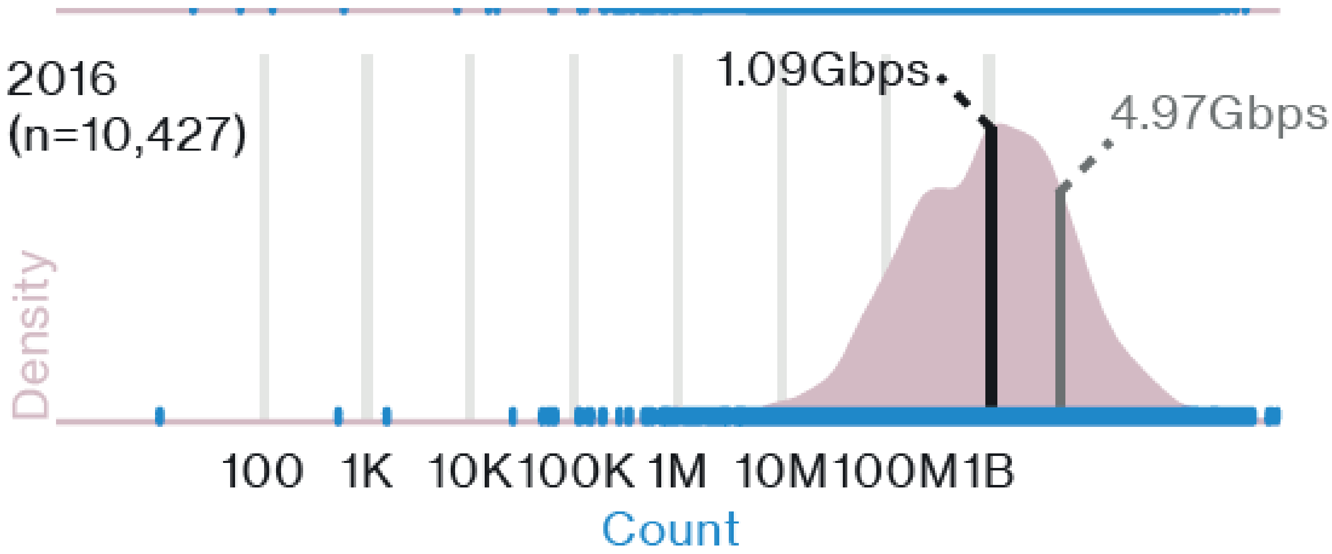
- Block executables at email gateway
- Disable macro-enabled Office docs if not needed
- Block JavaScript via email
- Keep browsers up to date
- Malware defenses
- Prioritize browser and plug-in exploitation patches

Web App Attacks Top Actions

- Common for web servers to attack different target
- Cross-site scripting and SQL injection haven’t disappeared but less favored than using credentials
- Minimize information or credentials on web server
- 2FA to slow intruders
- Patch CMS and plug-in consistently
- SQLi and input validation testing

Distributed denial-of-service (DDoS) attacks





DDoS Attacks Top Actions

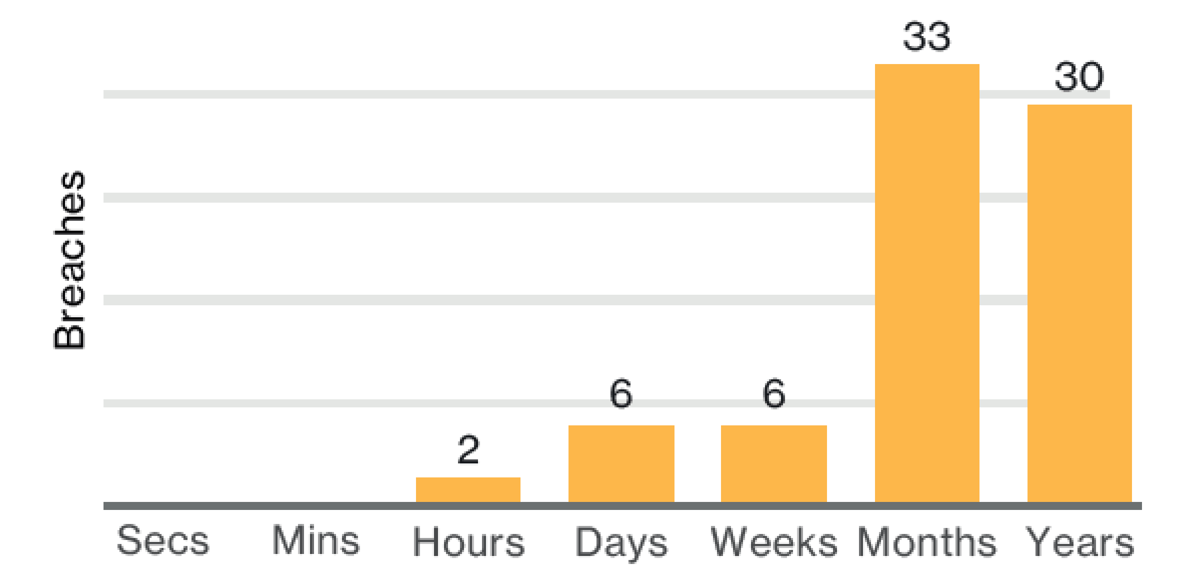
- Understanding mitigation needed is key
  - What attack length and size do you need to resist?
- Weigh business impact of not having defenses vs. cost of acquiring them

Physical Theft/Loss

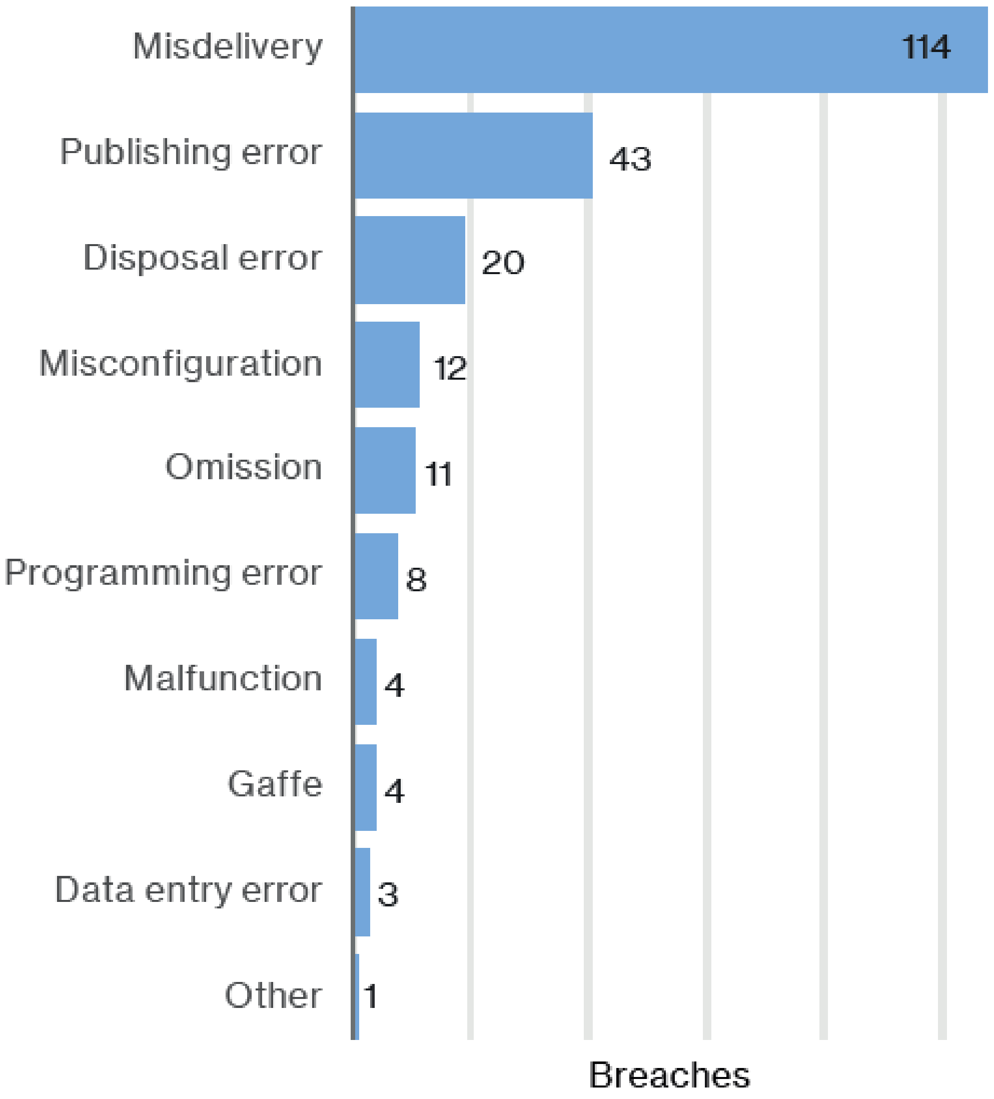
- Most theft occurred within victim’s work area and secondarily employee-owned vehicles
- Asset lost >> more often than stolen
- Encrypt and centrally manage
- Paper documents can’t be encrypted so handle sensitive data on a need to print basis or tokenize
- Train on data handling and monitor

Insider Misuse

- Top actions - privilege abuse for $ gain and curiosity
- Security controls identifying employee misuse detect external attackers masquerading as privileged users



Miscellaneous Errors



Miscellaneous Errors

- Directly leads to loss
- Need process for discarding anything sensitive
- Use past mistakes in security training for handling, storage, delivery and disposal
- Use 2nd reviewer for publishing reviewer
- Monitor webpages for publishing errors

Cyber-Espionage Top Actions

- Anti-malware at the email gateway
- Security awareness training
- Prioritize browser and plug-in exploitation patches
- Process to report phishing attempts with subsequent monitoring and logging
- Segment networks into zones requiring 2FA

Payment Card Skimmer Top Actions

- Gas pump terminals increase >3X from LY
- ATM incidents down 25% from LY
- Chip and pin slowly becoming prevalent
- Monitor outdoor terminals via video and review tapes
- Check as part of routine closing/opening
- Use tamper evident controls

Point of Sale Top Actions

- Defined by remote attacks against card transactions
- 95% of breaches with stolen credentials used vendor remote access to hack into their customer’s POS environments.
- POS vendors need to strengthen authentication and limit remote access

Everything Else

- Includes email compromises from management with wire transfer instructors requiring quick attention

Pre-texting email

From: Chris James CFO
Sent: Thursday, April 30, 2015 11:52 AM
To: Sam Watt, Controller
Subject: Fwd: Transfer

Sam,

Please process wire to the attached wire instruction accordingly. Code it to admin expenses and let me know when completed. I will send you details and invoice ASAP, you can use this email as backup for now if you need to.

Thanks,
Chris James, CFO

-------- Original Message --------
Subject: Transfer
Date: 2015-04-30 11:39 am
From: David Jones, President
To: Chris James, CFO
Copy: Bruce Davidson, Owner

Chris,

See attached wire instruction for the wire as discussed. Let me know when processed.

David Jones
President

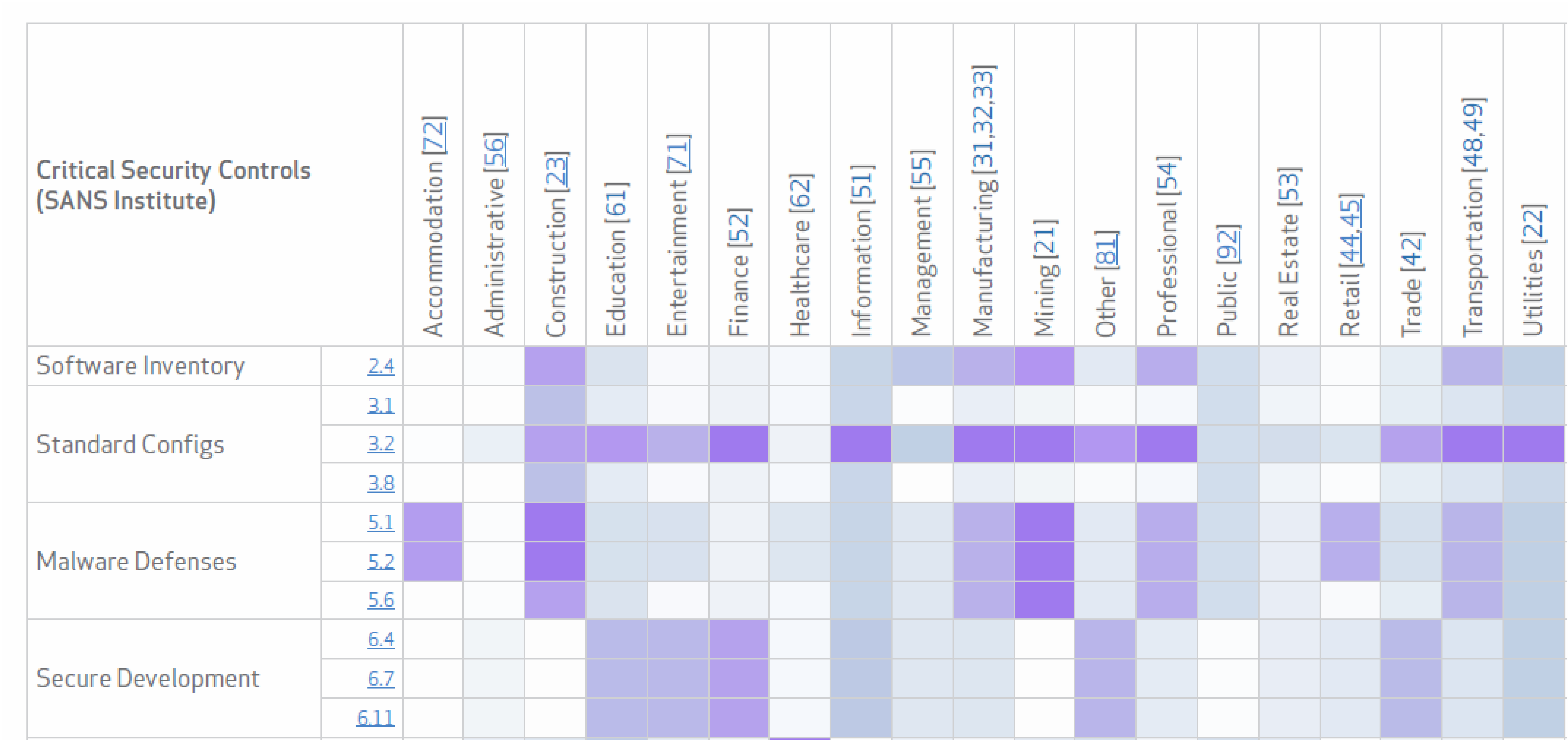
From: Ray Newton
[mailto:rnewton@syssrc.com]
Sent: Thursday, April 14, 2016 10:34 AM
To: Melanie Magness
Subject: SALARY REVIEW

Hello

I need you to send me all our employees 2015 W-2 (PDF) for an immediate review. I need you to attach them and send to me now.

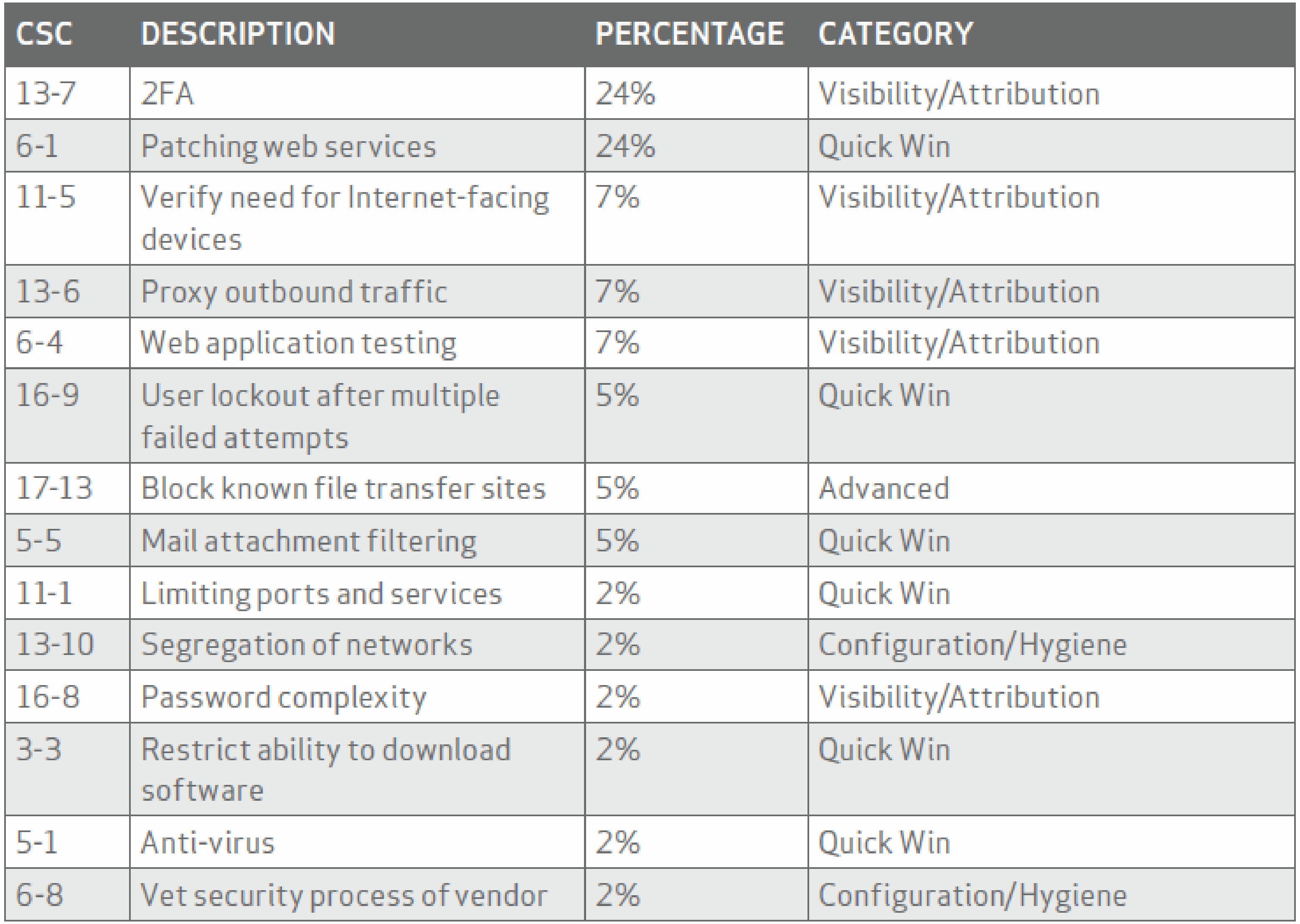
Thanks.

Actions - Prioritize Security Directions



Critical Security Controls (SANS Institute)		Accommodation [72]	Administrative [56]	Construction [23]	Education [61]	Entertainment [71]	Finance [52]	Healthcare [62]	Information [51]	Management [55]	Manufacturing [31,32,33]	Mining [21]	Other [81]	Professional [54]	Public [92]	Real Estate [53]	Retail [44,45]	Trade [42]	Transportation [48,49]	Utilities [22]
Software Inventory	2.4																			
Standard Configs	3.1																			
	3.2																			
	3.8																			
Malware Defenses	5.1																			
	5.2																			
	5.6																			
Secure Development	6.4																			
	6.7																			
	6.11																			

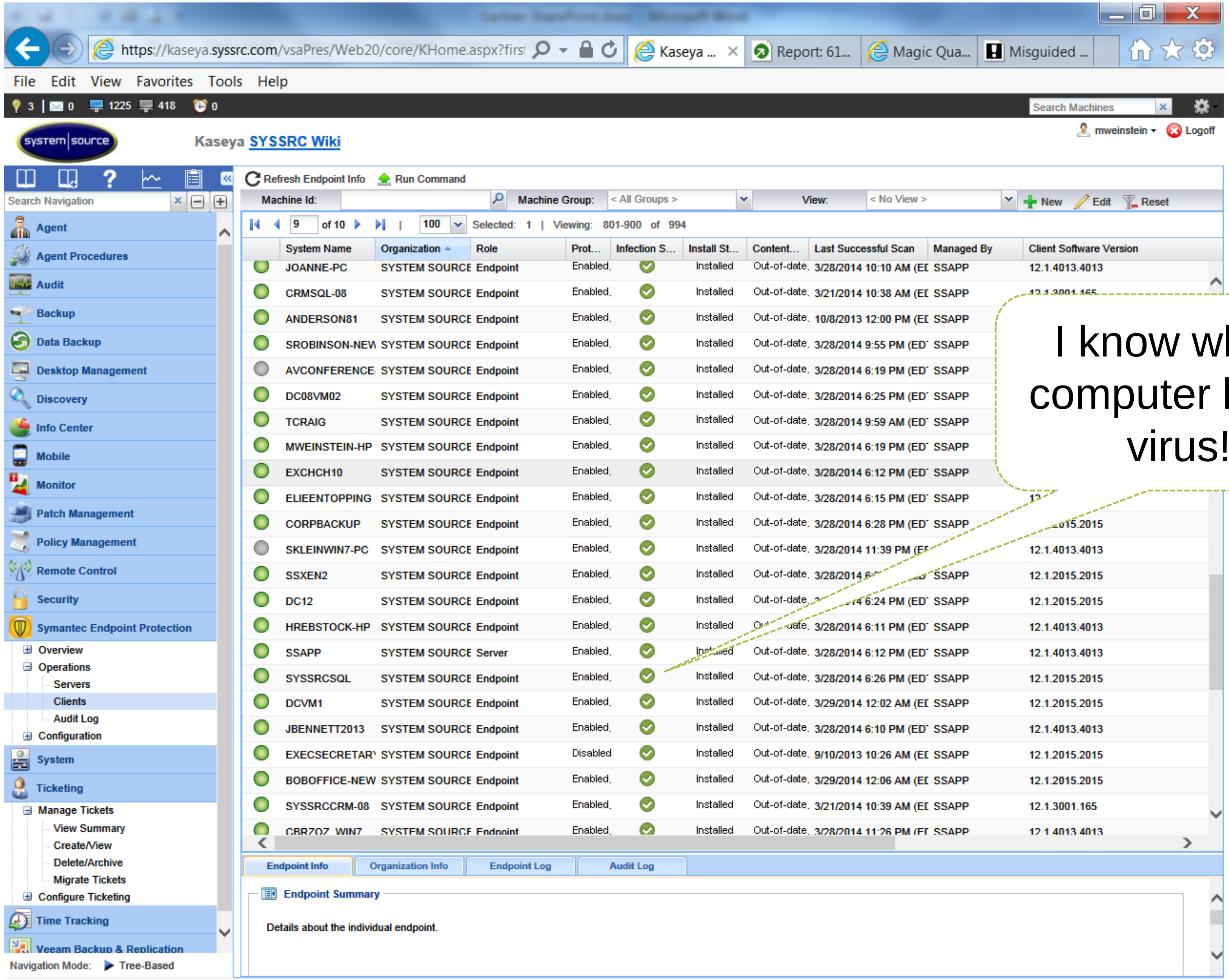
% incidents where a CSC control is recommended



CSC	DESCRIPTION	PERCENTAGE	CATEGORY
13-7	2FA	24%	Visibility/Attribution
6-1	Patching web services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file transfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download software	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

40% of “most effective” controls are in the “Quick Win” category

Action - Proactivity Drives Risk Reduction



Kaseya SYSSRC Wiki

Machine Id: Machine Group: < All Groups > View: < No View >

9 of 10 | 100 Selected: 1 | Viewing: 801-900 of 994

	System Name	Organization	Role	Prot...	Infection S...	Install St...	Content...	Last Successful Scan	Managed By	Client Software Version
●	JOANNE-PC	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 10:10 AM (EI	SSAPP	12.1.4013.4013
●	CRMSQL-08	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/21/2014 10:38 AM (EI	SSAPP	12.1.3001.165
●	ANDERSON81	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	10/8/2013 12:00 PM (EI	SSAPP	
●	SROBINSON-NEW	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 9:55 PM (ED	SSAPP	
○	AVCONFERENCE-	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:19 PM (ED	SSAPP	
●	DC08VM02	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:25 PM (ED	SSAPP	
●	TCRAIG	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 9:59 AM (ED	SSAPP	
●	MWEINSTEIN-HP	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:19 PM (ED	SSAPP	
●	EXCHCH10	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:12 PM (ED	SSAPP	
●	ELIEENTOPPING	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:15 PM (ED	SSAPP	12
●	CORPBACKUP	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:28 PM (ED	SSAPP	015.2015
○	SKLEINWIN7-PC	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 11:39 PM (EI		12.1.4013.4013
●	SSXEN2	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:	SSAPP	12.1.2015.2015
●	DC12	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	14 6:24 PM (ED	SSAPP	12.1.2015.2015
●	HREBSTOCK-HP	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:11 PM (ED	SSAPP	12.1.4013.4013
●	SSAPP	SYSTEM SOURCE	Server	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:12 PM (ED	SSAPP	12.1.4013.4013
●	SYSSRCSQL	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:26 PM (ED	SSAPP	12.1.2015.2015
●	DCVM1	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/29/2014 12:02 AM (EI	SSAPP	12.1.2015.2015
●	JBENNETT2013	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 6:10 PM (ED	SSAPP	12.1.4013.4013
●	EXECSECRETARY	SYSTEM SOURCE	Endpoint	Disabled	✓	Installed	Out-of-date.	9/10/2013 10:26 AM (EI	SSAPP	12.1.2015.2015
●	BOBOFFICE-NEW	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/29/2014 12:06 AM (EI	SSAPP	12.1.2015.2015
●	SYSSRCCRM-08	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/21/2014 10:39 AM (EI	SSAPP	12.1.3001.165
●	CBRZOZ_WIN7	SYSTEM SOURCE	Endpoint	Enabled.	✓	Installed	Out-of-date.	3/28/2014 11:26 PM (EI	SSAPP	12.1.4013.4013

Endpoint Summary

Details about the individual endpoint.

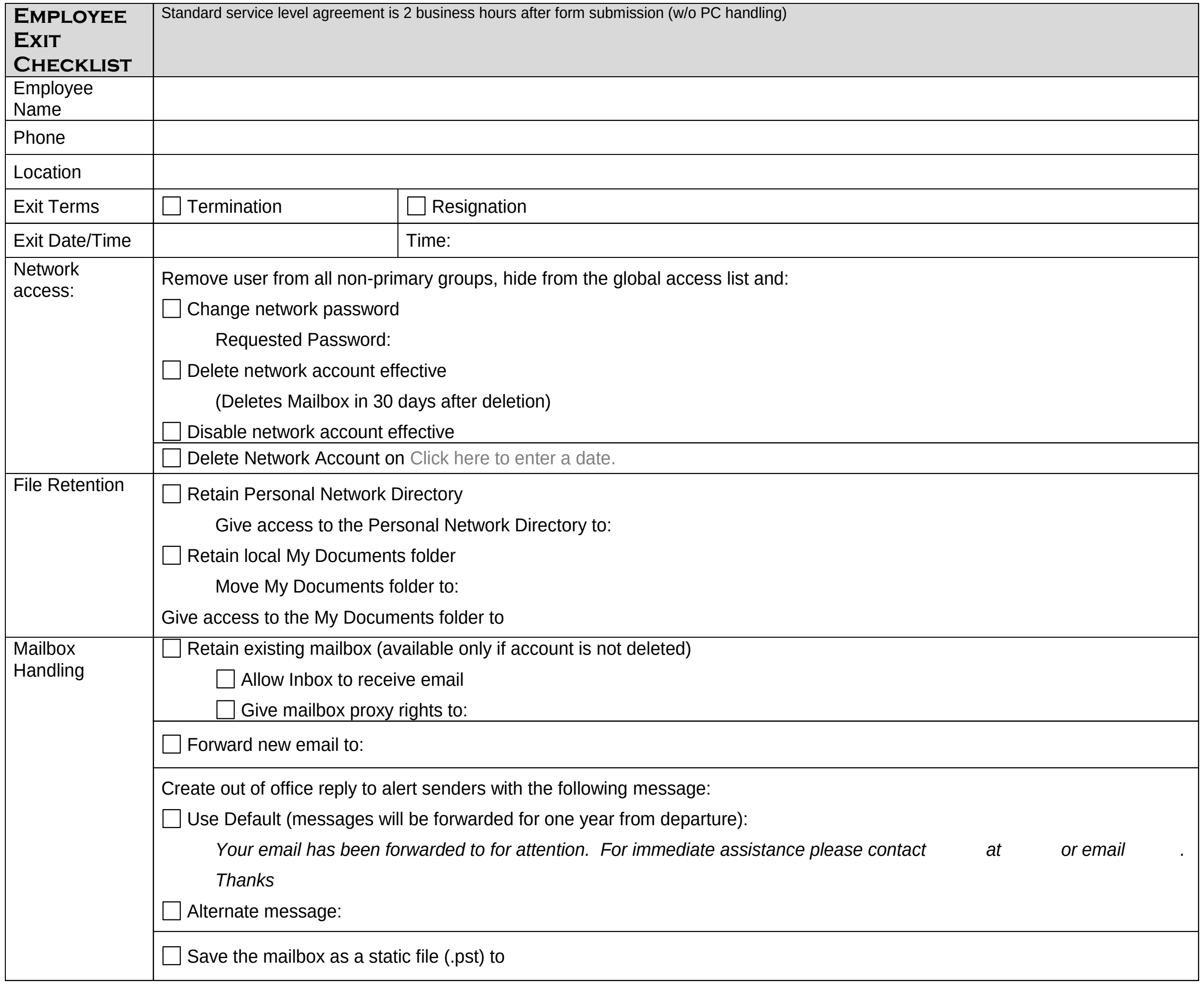
I know which computer has a virus!

Actionable Security Reports

- User accounts with escalated administrative privileges
- User accounts not logged in within the last 90 days
- Computers not connected to the domain in >90 days
- Computers running outdated operating systems (Server 2003 and XP)
- Proofpoint spam filtering and spooling report
- SEP risk report
- Report showing passwords not changed in 90 days
- Password policy
- Log retention policy settings
- Account lockout monitoring
- Bad password attempt monitoring
- Office 365 last logon
- Screen lock settings

Action- Staff Entrance and Exit

Detailed procedures onboard/exit new staff efficiently



EMPLOYEE EXIT CHECKLIST	Standard service level agreement is 2 business hours after form submission (w/o PC handling)	
Employee Name		
Phone		
Location		
Exit Terms	□ Termination	□ Resignation
Exit Date/Time		Time:
Network access:	Remove user from all non-primary groups, hide from the global access list and: □ Change network password Requested Password: □ Delete network account effective (Deletes Mailbox in 30 days after deletion) □ Disable network account effective	
	□ Delete Network Account on Click here to enter a date.	
File Retention	□ Retain Personal Network Directory Give access to the Personal Network Directory to: □ Retain local My Documents folder Move My Documents folder to: Give access to the My Documents folder to	
Mailbox Handling	□ Retain existing mailbox (available only if account is not deleted) □ Allow Inbox to receive email □ Give mailbox proxy rights to:	
	□ Forward new email to:	
	Create out of office reply to alert senders with the following message: □ Use Default (messages will be forwarded for one year from departure): *Your email has been forwarded to for attention. For immediate assistance please contact at or email .* *Thanks* □ Alternate message:	
	□ Save the mailbox as a static file (.pst) to	

Ask About IT

Evaluations & Door Prizes

THANK YOU!