Nasty Nine Information Security Mistakes

Peter Tippett
CEO, HealthCelerate
Chairman, DataMotion

The Nasty Nine:

1. Risk is most related to vulnerability
2. The best way to reduce risk: implement stronger solutions, policies & training
3. Apply Security Patches Faster for zero day and wildfire increases in risk each time new vulnerabilities are published
4. Encryption data in transit is among top 10 most important controls
   Encryption data at rest is among strongest controls for servers
5. Use Stronger Passwords to reduce risk
6. Use Stronger Identity Proofing to reduce risk
7. HIPAA security standard has a lot of onerous requirements and is among the most complex & difficult to achieve certification
8. Intrusion Detection Systems (IDS) are a relatively efficient and effective
9. Mobile and IoT are the new Big Risks

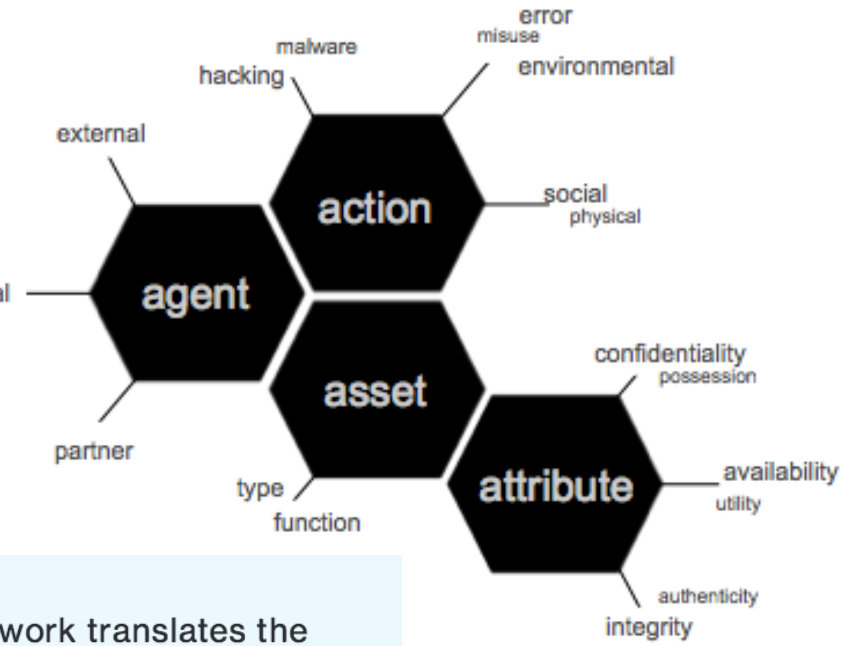
9 Years of Data Breach Investigations Reports (DBIR) >100,000 incidents, 2,260 breaches in 2016 dataset, <12k all years

An ongoing study into the world of cybercrime that analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and, of course, what might be done to prevent it.

Available at http://www.verizonenterprise.com/DBIR/
http://securityblog.verizonbusiness.com

VERIS Framework

VERIS is a (open and free) set of metrics designed to provide a common language for describing security incidents (or threats) in a structured and repeatable manner.



Classifying incidents using VERIS

The incident classification section of the VERIS framework translates the incident narrative of "who did what to what (or whom) with what result" into a form more suitable for trending and analysis. To accomplish this, VERIS employs the A4 Threat Model developed by Verizon's RISK Team. In the A4 model, a security incident is viewed as a series of events that adversely affects the information assets of an organization. Every event is comprised of the following elements (the four A's):

- **Actor**–Whose actions affected the asset
- **Action**–What actions affected the asset
- **Asset**–Which assets were affected
- **Attribute**–How the asset was affected

It is our position that the four A's represent the minimum information necessary to adequately describe any incident or threat scenario. Furthermore, this structure provides an optimal framework within which to measure frequency, associate controls, link impact and many other concepts required for risk management.

#1 Risk is most related to vulnerability

Define Risk in a Measurable Way

The RISK EQUATION:

Business Risk =

Threat * **Vulnerability** * **Impact**

(freq of attempts) (likelihood of success) ($ if successful)

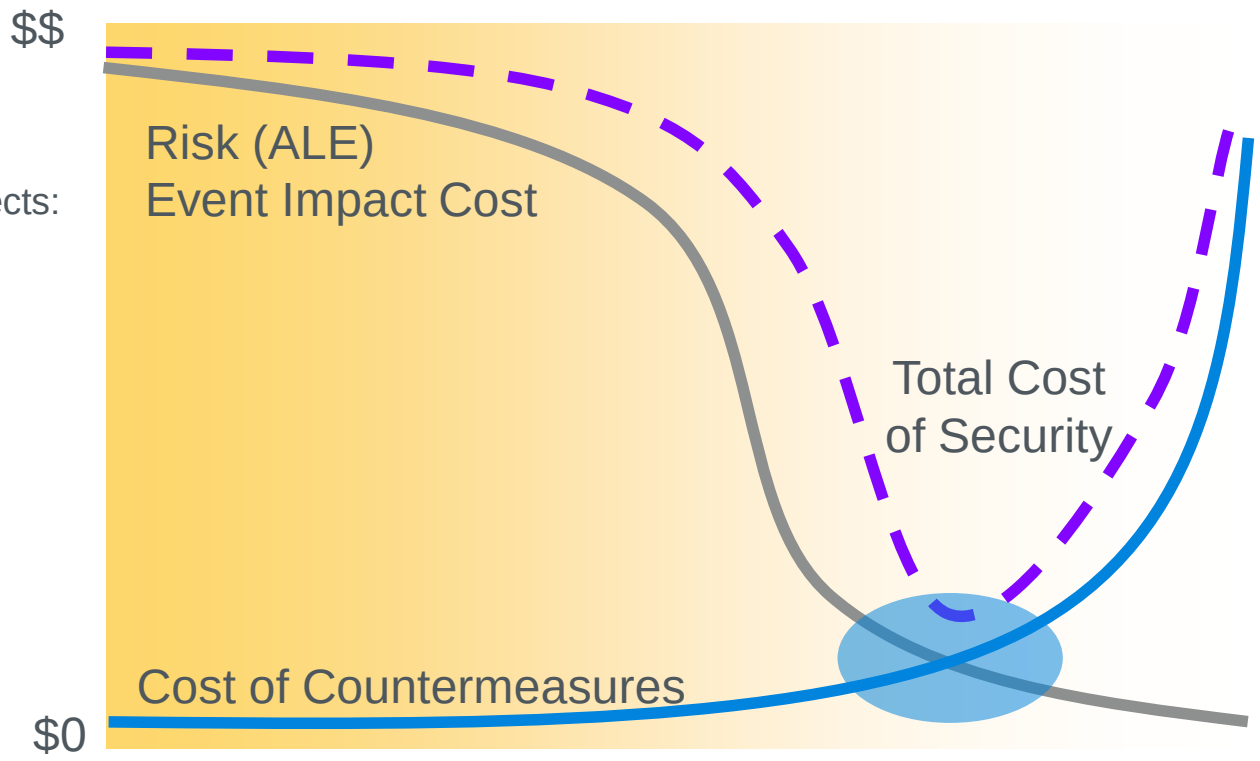
Business Risk = ALE

Annualized Loss Expectancy ($/yr)

Goal: Improve Enterprise Profit

Potential Values of Information Security Projects:

- Reducing Future Losses ($$ ALE)
- Reducing Spending ($)
- Increasing Revenue ($)



Impact (Cost Per Breached Record)

All industries

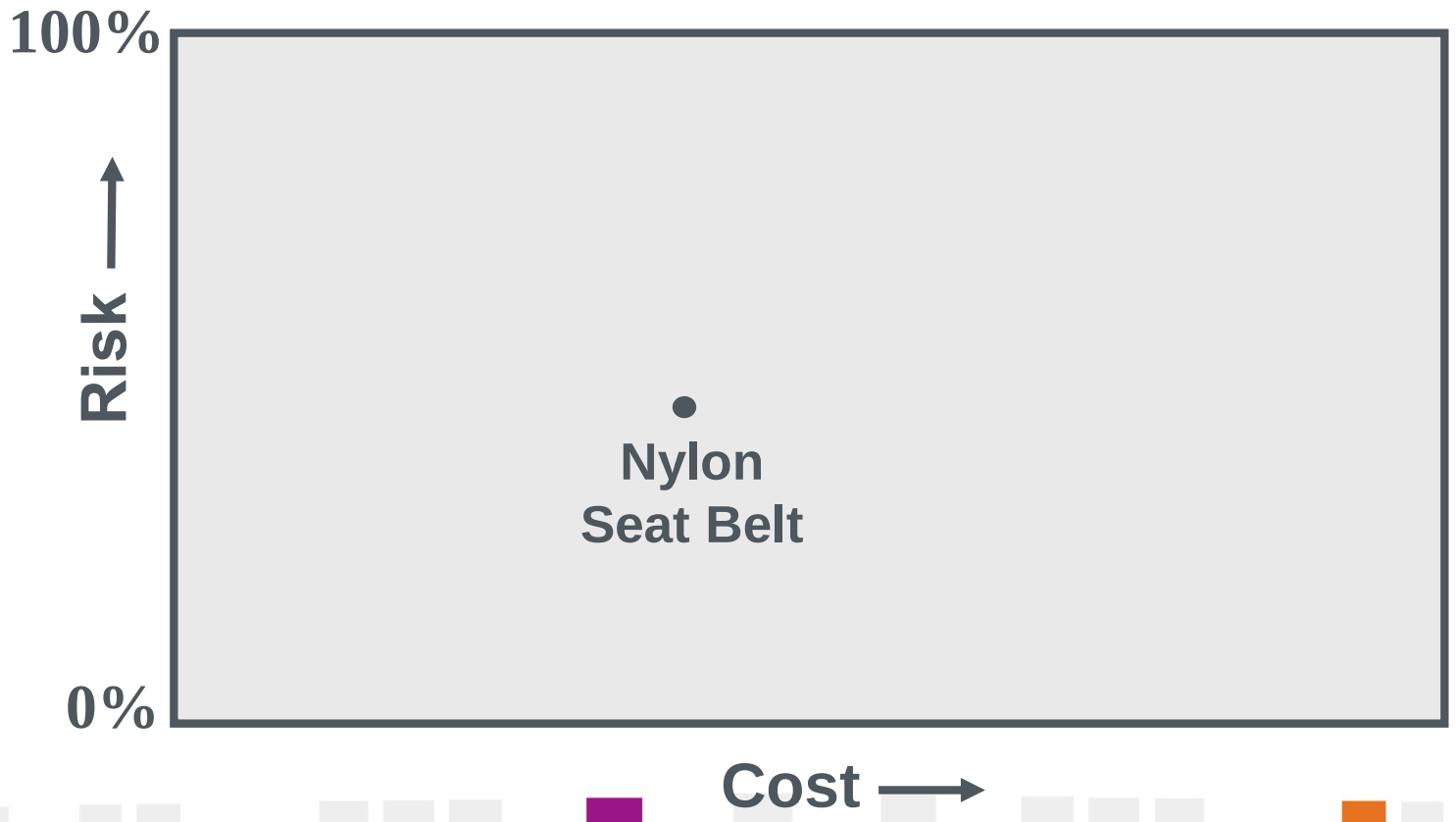
If we had $201 for every time someone asked us, "Do you have data on the cost of breaches?", we'd have $128,037.[29] For the past seven years, we've had to answer that question with an apologetic "No," while doing our best to explain why.[30] But not this time; we're absolutely ecstatic to offer an anticipatory "Yes!" to that question in this long-overdue section. It took us eight years to get here, but "better eight than never," right?

Our approach to estimating loss is based on actual data and considers multiple contributing factors—not just number of records.

2) The best way to reduce risk: implement stronger solutions, policies & training…

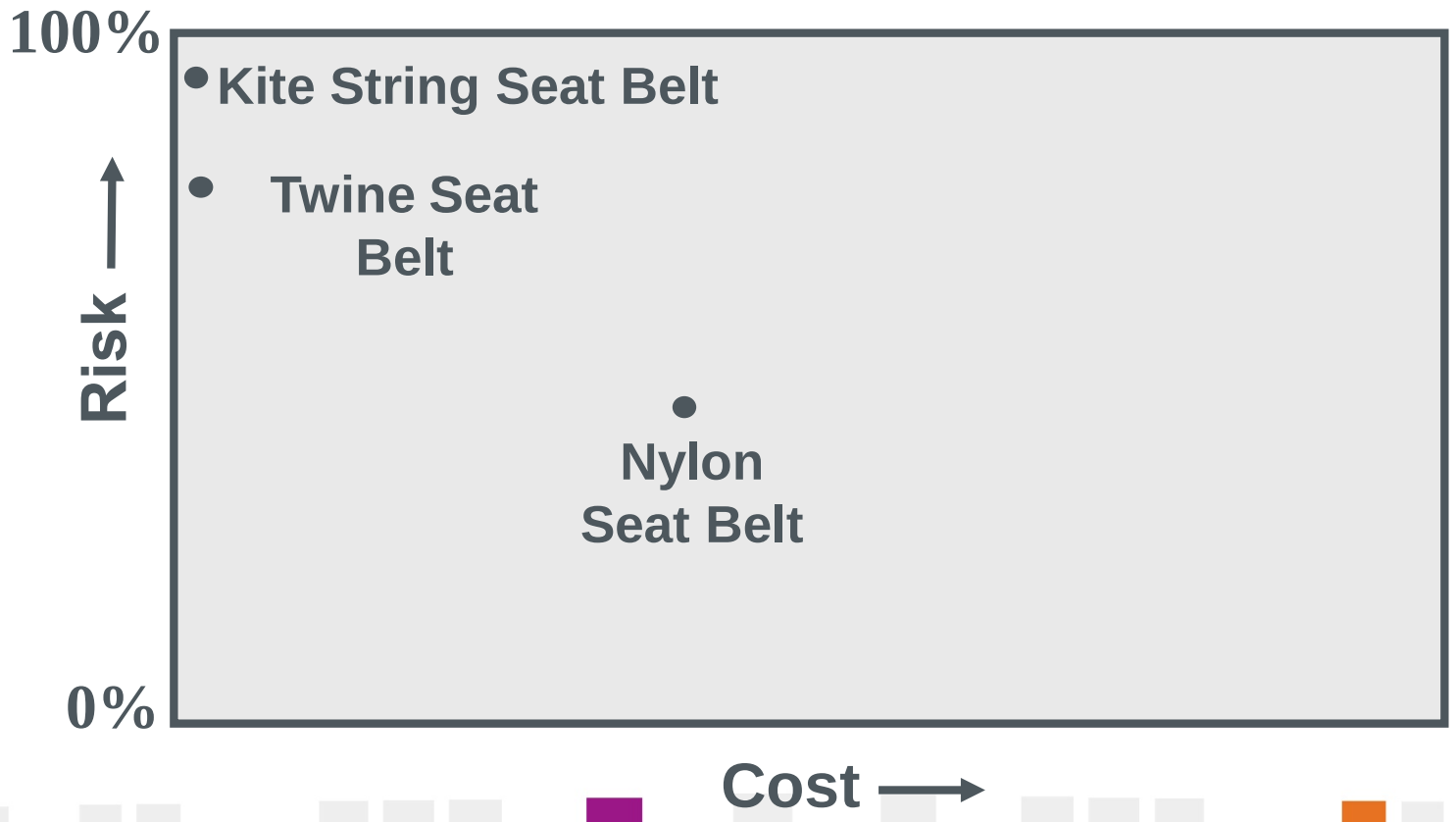
A Simple Thought Experiment

Risk Equation: Risk ($/yr) = Threat * Vulnerability * Impact



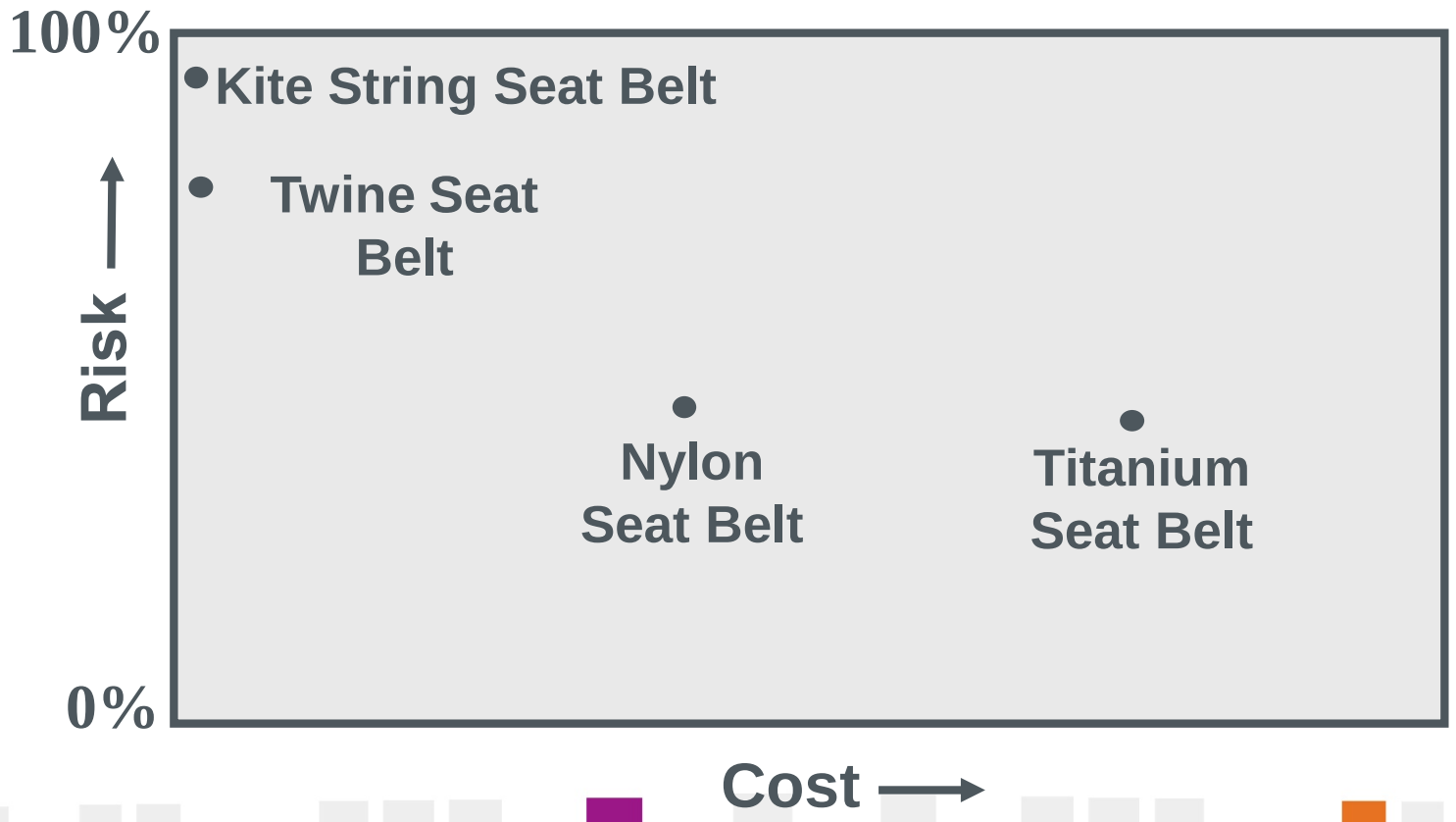
A Simple Thought Experiment

Risk Equation: Risk ($/yr) = Threat * Vulnerability * Impact

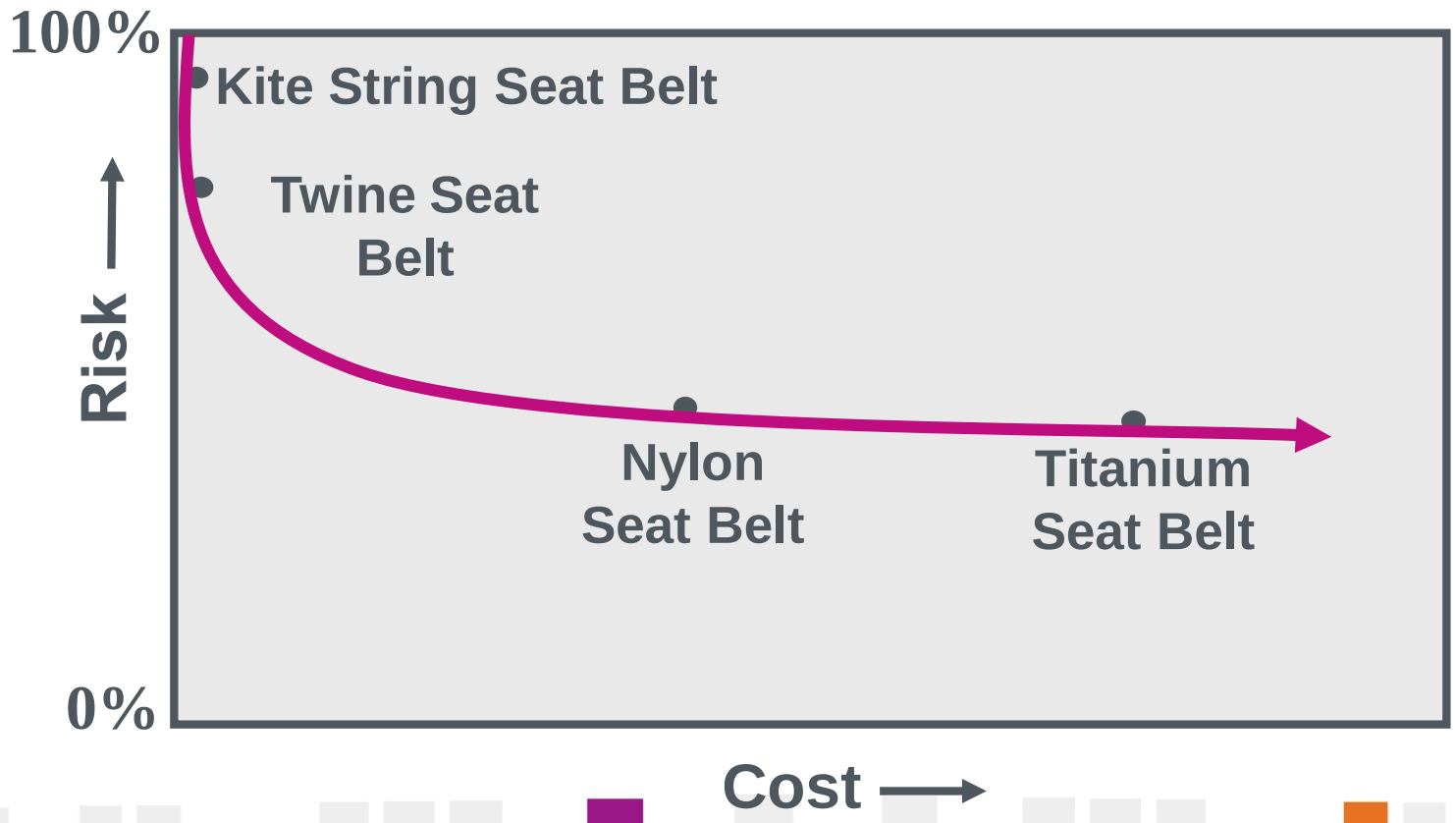


A Simple Thought Experiment

Risk Equation: Risk ($/yr) = Threat * Vulnerability * Impact

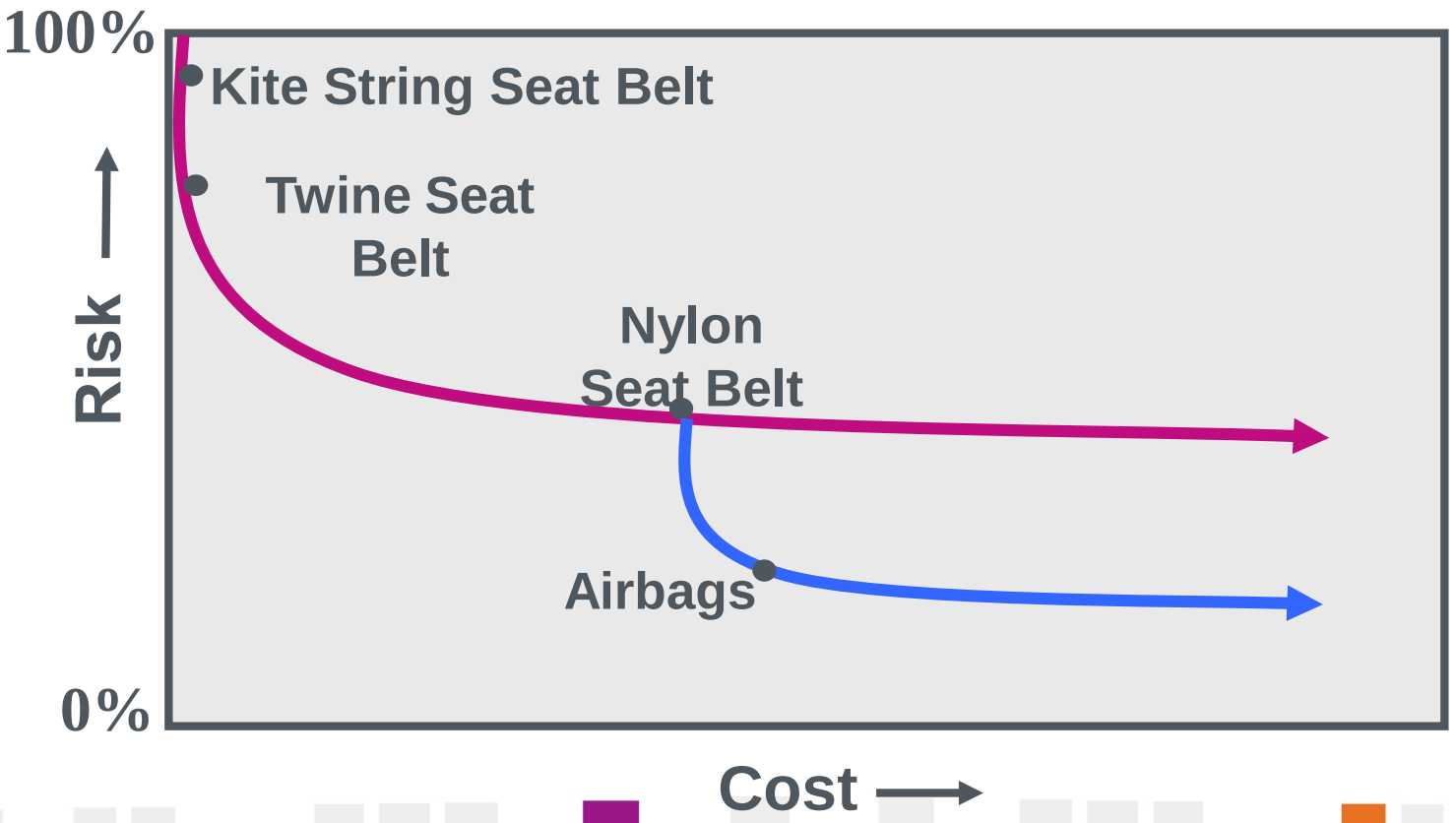


A Simple Thought Experiment



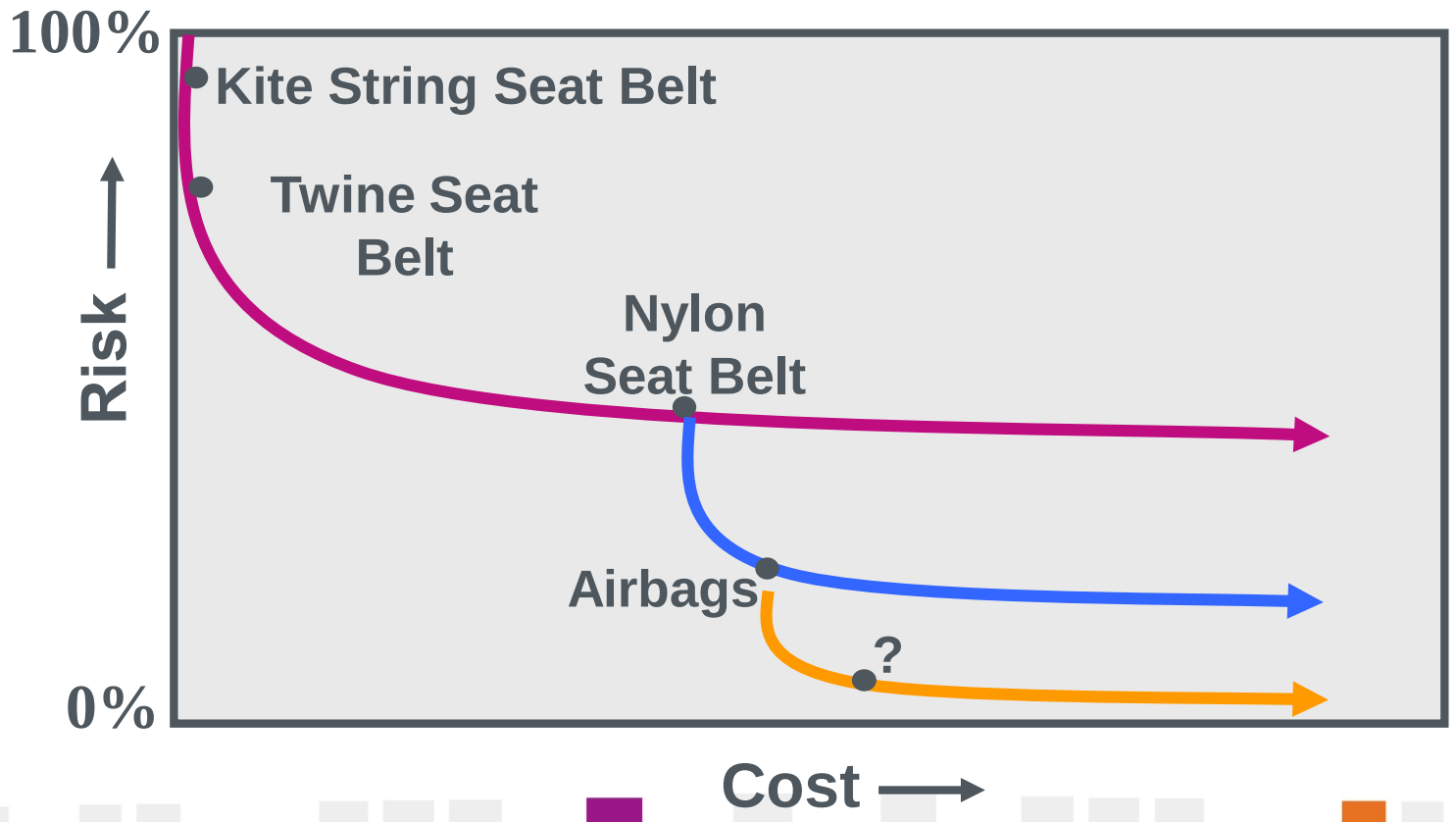
A Simple Thought Experiment

Risk Equation: Risk ($/yr) = Threat * Vulnerability * Impact



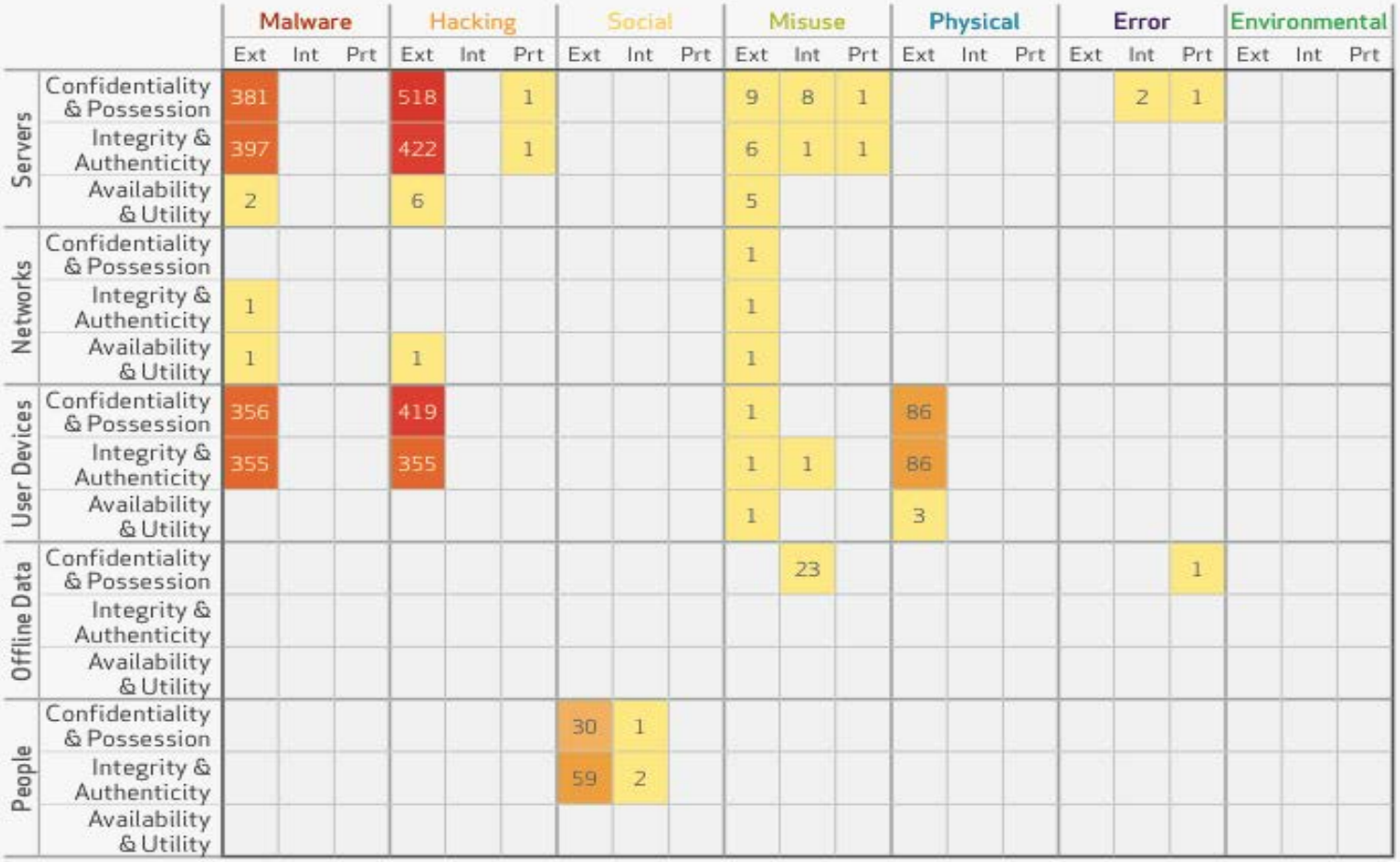
A Simple Thought Experiment

Risk Equation: Risk ($/yr) = Threat * Vulnerability * Impact



Frequency high level events across all of VERIS framework

Figure 8. VERIS A⁴ Grid depicting the frequency of high-level threat events



		Malware			Hacking			Social			Misuse			Physical			Error			Environmental		
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
Servers	Confidentiality & Possession	381			518		1				9	8	1					2	1			
	Integrity & Authenticity	397			422		1				6	1	1									
	Availability & Utility	2			6						5											
Networks	Confidentiality & Possession										1											
	Integrity & Authenticity	1									1											
	Availability & Utility	1			1						1											
User Devices	Confidentiality & Possession	356			419						1			86								
	Integrity & Authenticity	355			355						1	1		86								
	Availability & Utility										1			3								
Offline Data	Confidentiality & Possession											23							1			
	Integrity & Authenticity																					
	Availability & Utility																					
People	Confidentiality & Possession							30	1													
	Integrity & Authenticity							59	2													
	Availability & Utility																					

3) Apply Security Patches Faster

The Data - Better to patch everything slowly than anything fast

All industries

99.9%
OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.

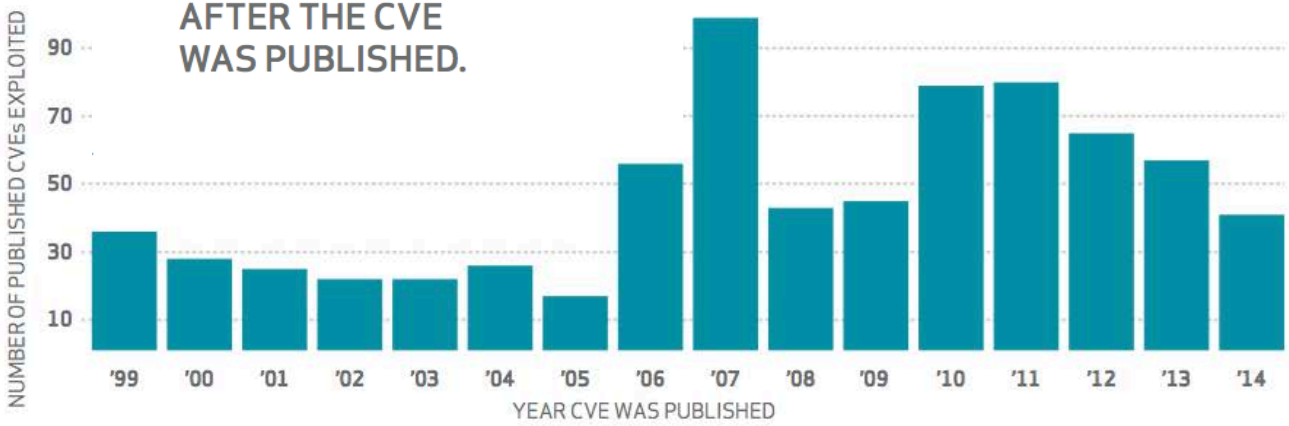


Figure 10.

Count of exploited CVEs in 2014 by CVE publish date

11 Common Vulnerabilities and Exposures (CVE) is "a dictionary of publicly known information security vulnerabilities and exposures."—cve.mitre.org

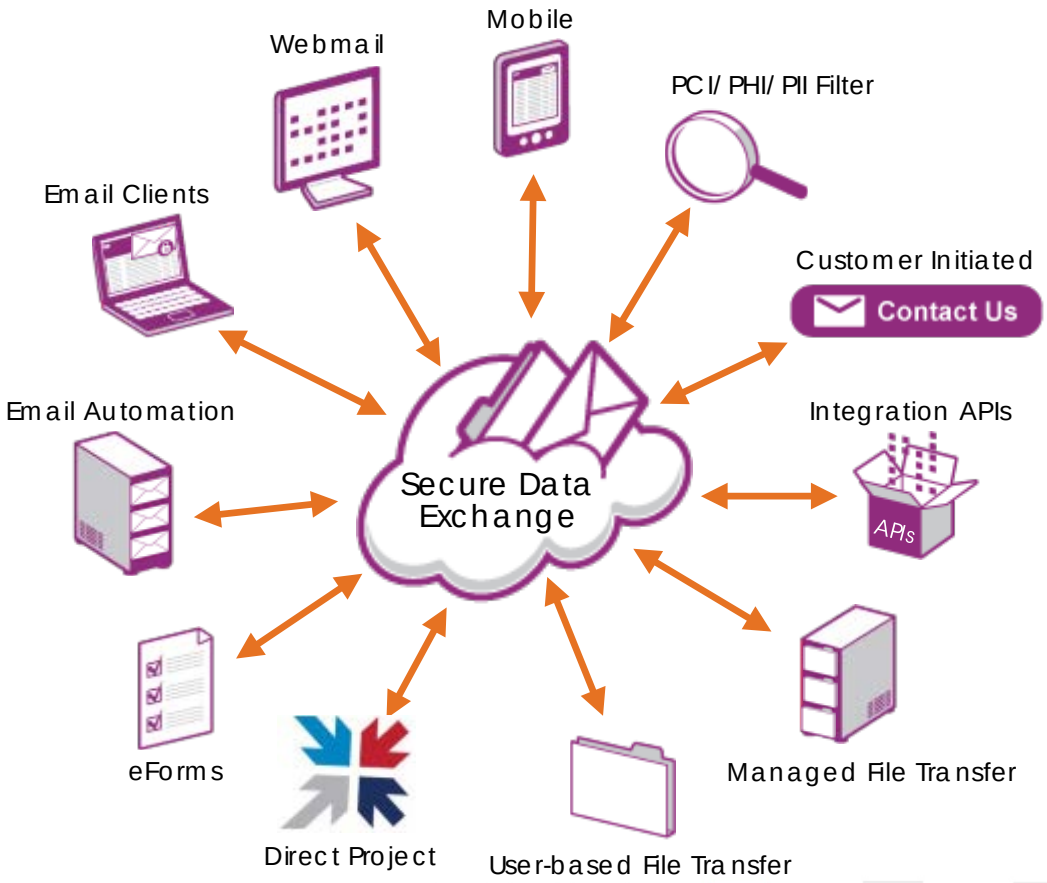
#4 Encryption

Encryption data in transit is among top 10 most important controls

Encryption data at rest is among strongest controls for servers

The DataMotion Software Platform

‘Hub and Spoke Design’ Delivering all DataMotion secure solutions!



- Core Encryption Engine
- Optimized for Mobile, Web and Desktop Client Access
- Architected for Cloud, Premise or Hybrid Deployment
- Supports a wide range of workflows
- Strategic asset to an organization
- Consistent compliance across the organization
- Consistent admin and user experience
- Extensible without losing security

Top Threat Actions Over Time

All industries

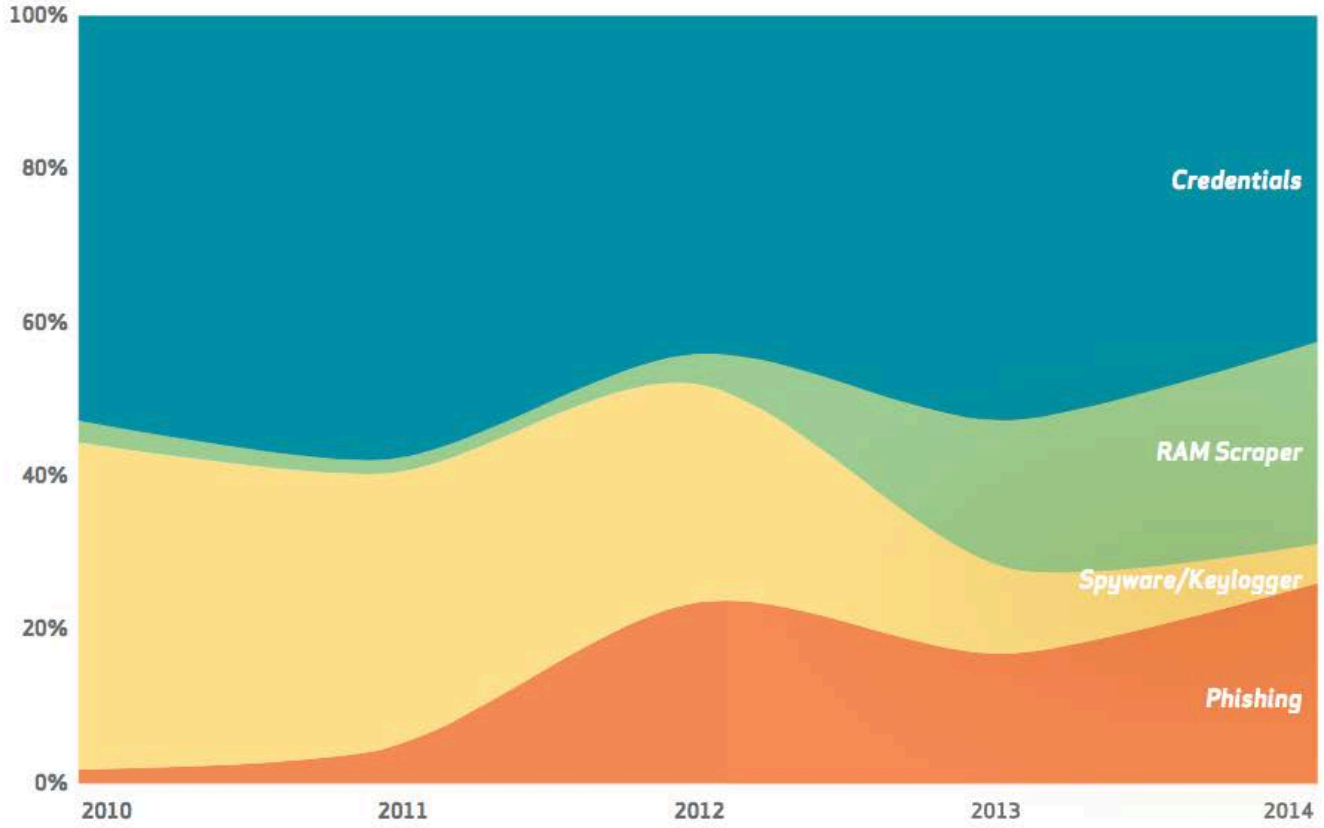


Figure 4.

Significant threat actions over by percent

Top Threat Actions Over Time Detail from 2016 Data

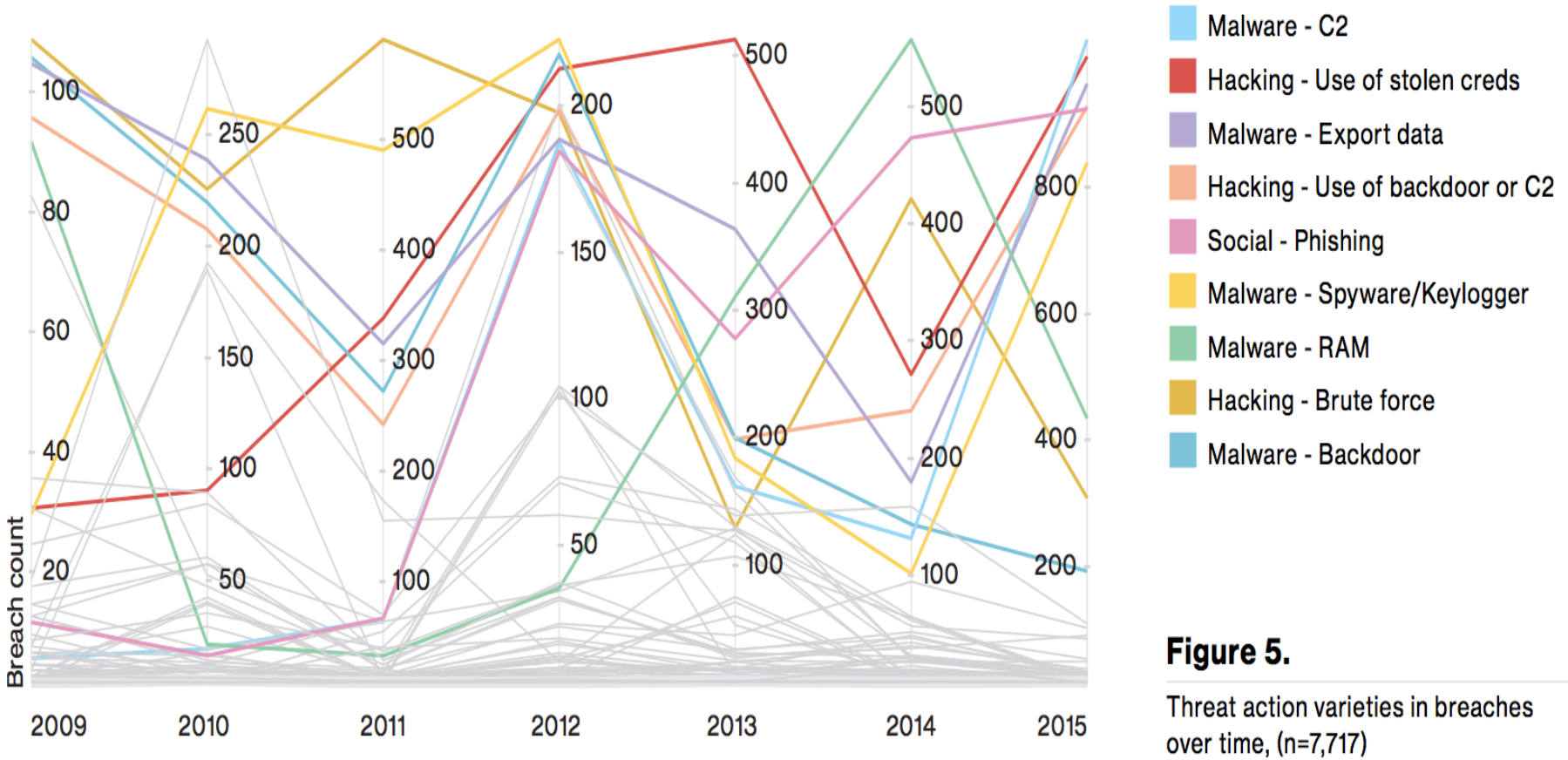


Figure 5.

Threat action varieties in breaches over time, (n=7,717)

#5) Use Stronger Passwords to reduce risk

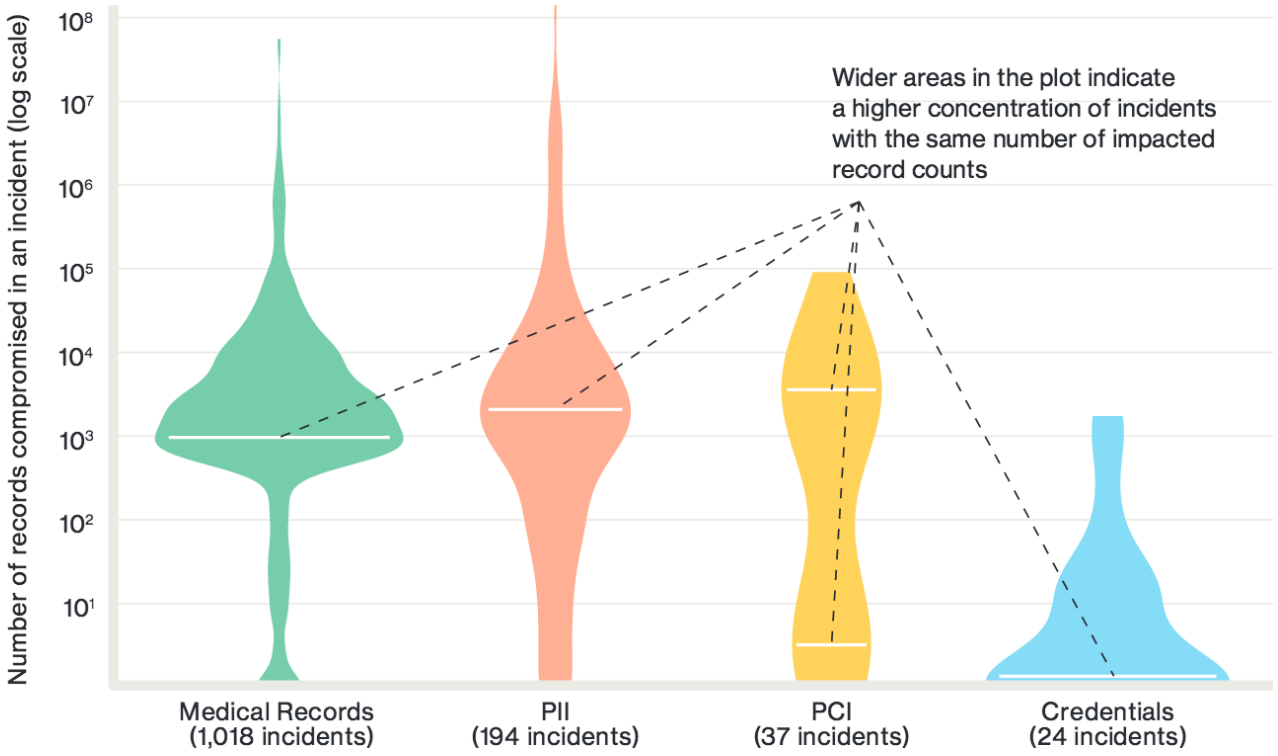
	4	~6	8	10	12
1	root	ADMIN	password	1234567890	abcdefghijkl
2	Root	Admin	Password	Passw0rd1#	-Passw0rd#1/
3	Abc1	o!2345	Qwerty#1		
4	A1a!	AaSs12!@	QWERty1!		
4R	0,hI	#E5g^h	9,J5%x}b	9x(v*B6r$z	7e6X@Gi(wV:4

#5) Use Stronger Passwords to reduce risk

	4	~6	8	10	12
1	root	ADMIN	password	1234567890	abcdefghijkl
2	Root	Admin	Password	Passw0rd1#	-Passw0rd#1/
3	Abc1	o!2345	Qwerty#1		
4	A1a!	AaSs12!@	QWERty1!		
4R	0,hI	#E5g^h	9,J5%x}b	9x(v*B6r$z	7e6X@Gi(wV:4

	F) Fire the person	**W)** Weak password	**G)** Good Password	**S)** Strong password
Definition	Exceedingly common failure in real world	Would fail against >80% of real world attacks	Would protect against more than half of real-world attacks	Would protect against more than >95% of real-world attacks
Attacks against Admin on Servers				
Attacks against User accounts on Servers				
Attacks against lost Laptop/mobile				

Data Types Disclosed Health Sector



In the common scenario where a database record contains medical information as well as PII, the incident is classified as "medical records."

Figure 4.

Data types disclosed

#6) Use Stronger Identity Proofing to reduce risk

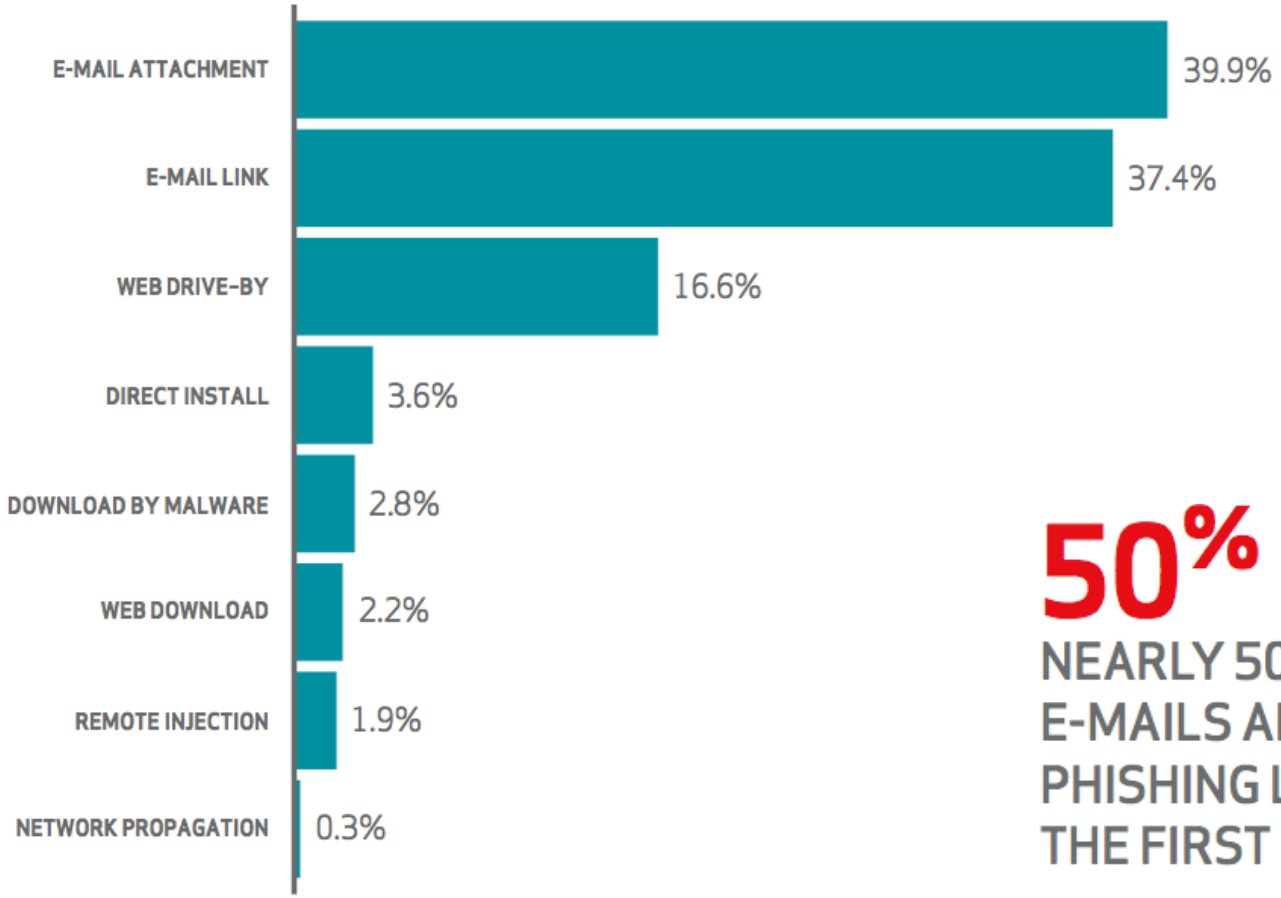
- Two Factor Authentication Fixes all of this
- Stronger proofing would have prevented zero (possibly one case) of the 79,000 successful attacks in the DBIR

#7) HIPAA security standard has a lot of onerous requirements and is among the most complex & difficult to achieve certification

- HIPAA Security Rule
  - » Encrypt data in transit
  - » Consider encrypting data in storage
  - » Do good identity proofing of those accessing data
  - » Log everything well
  - » Contractually oblige others who share or manipulate data to “due care” (BAA)
  - » Do a Risk Assessment
  - » Address the Risk from the Risk Assessment

Vector for malware installation

All industries

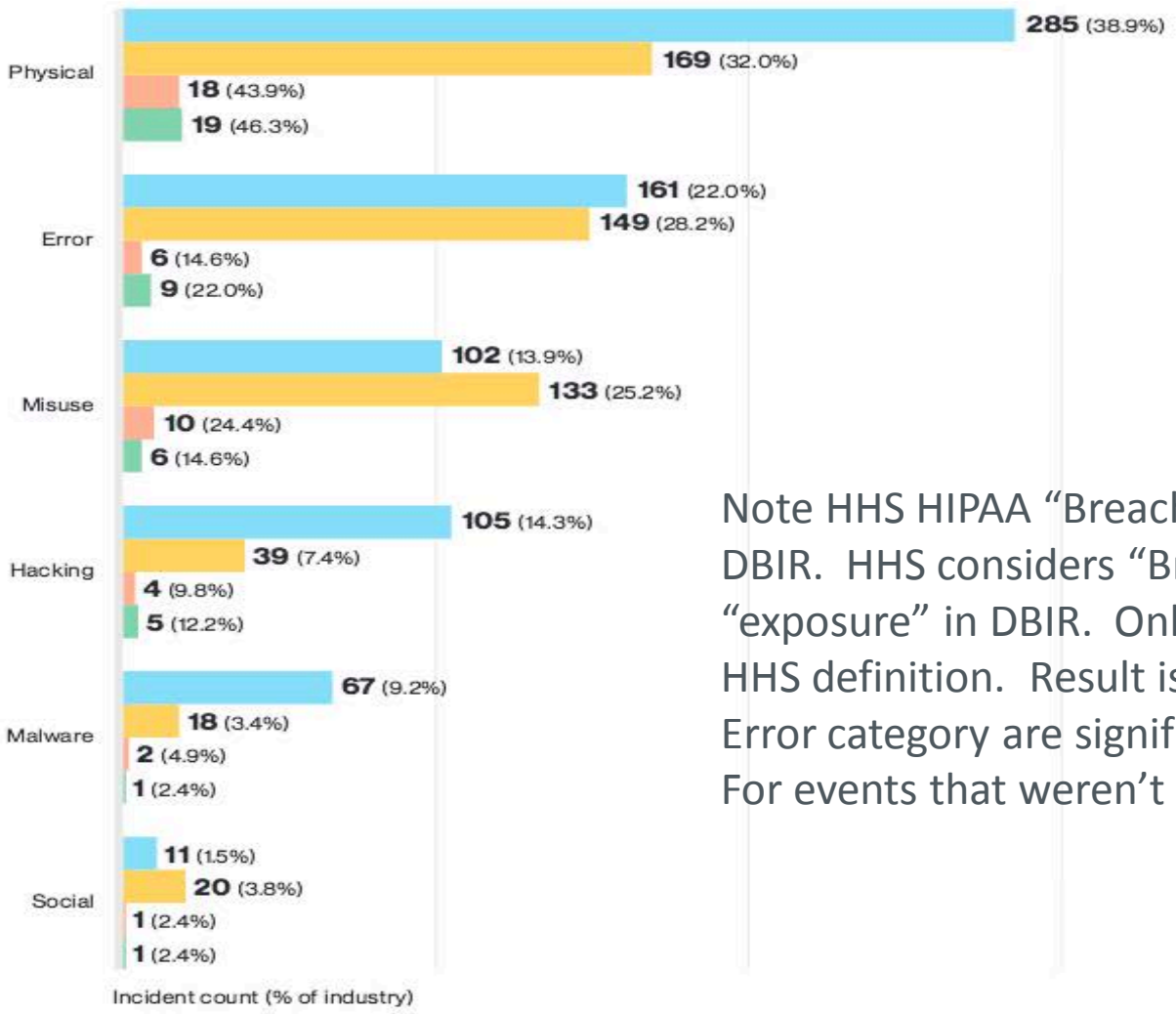


50%

NEARLY 50% OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

Vector of malware installatic

Threat Actions in Health Industry



The healthcare industry is divided into four separate three-digit NAICS codes:

- 621 – Ambulatory healthcare services (includes all types of doctor and dentist offices)
- 622 – Hospitals
- 623 – Nursing and residential care facilities
- 624 – Social assistance

Note HHS HIPAA "Breach" definition differs from DBIR. HHS considers "Breach" the same as an "exposure" in DBIR. Only the 2015 PHI DBIR uses the HHS definition. Result is Physical and much of Error category are significantly over-represented For events that weren't really breaches.

Figure 8.
Actions by three-digit NAICS code

Drill down on Error Actions Health sector

- **Loss**—Loss or misplacement of an asset.
- **Misdelivery**—Whether it is documents in the mail or electronic information in e-mail, it amounts to people getting data they weren't supposed to.
- **Disposal errors**—Primarily paper documents, but also electronic devices containing sensitive information.
- **Publishing errors**—When private information gets posted to an Internet-facing system and then is indexed by search engines.

For lost or even stolen devices, it is critical to ensure the organization has an easy way for people to report these incidents quickly. The sooner you know, the faster you can react to the breach.

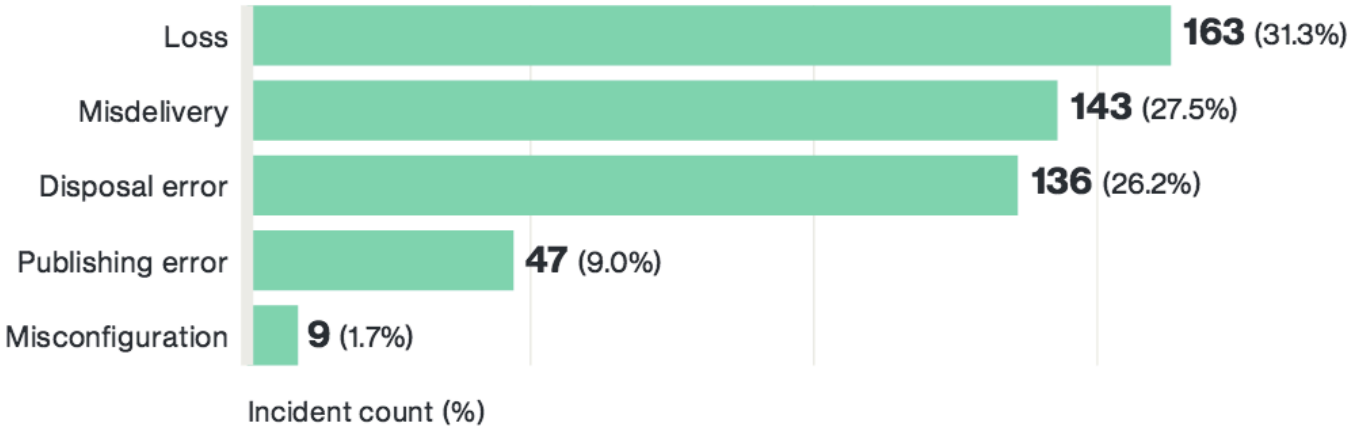
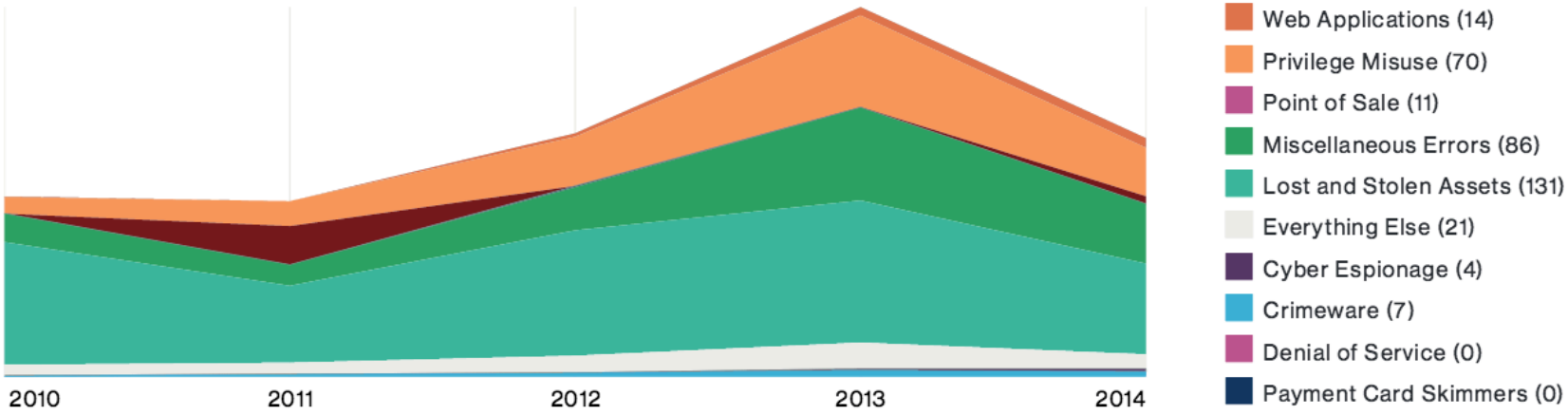


Figure 13.

Error Action top five

9 breach patterns over time Health Sector

The nine patterns over time
Looking at the trend of the nine patterns over time (Figure 14) shows how the mix has changed. The Internal Actor (Privilege Misuse) has been a constant companion for organizations in this dataset, but you can see how it really took off in 2013. Web Applications attacks have also seen a steady growth over the years, whereas the Point of Sale attack appeared to not be an issue in 2013, but has since enjoyed a mini-renaissance.



You can see the dominance of the Lost and Stolen Assets pattern through the years for this dataset. There hasn't been much progress on mitigating that risk, and it has seen a steady growth. The Miscellaneous Errors pattern also saw a jump in 2013, but has dropped some since then. However, we don't think people are going to stop making mistakes any time soon, so it is a safe bet that pattern will be in it for the long haul.

Figure 14.
Number of breaches by pattern over time

#8) Intrusion Detection Systems (IDS) are a relatively efficient and effective

Attacks happen fast, Discovering them is usually slow

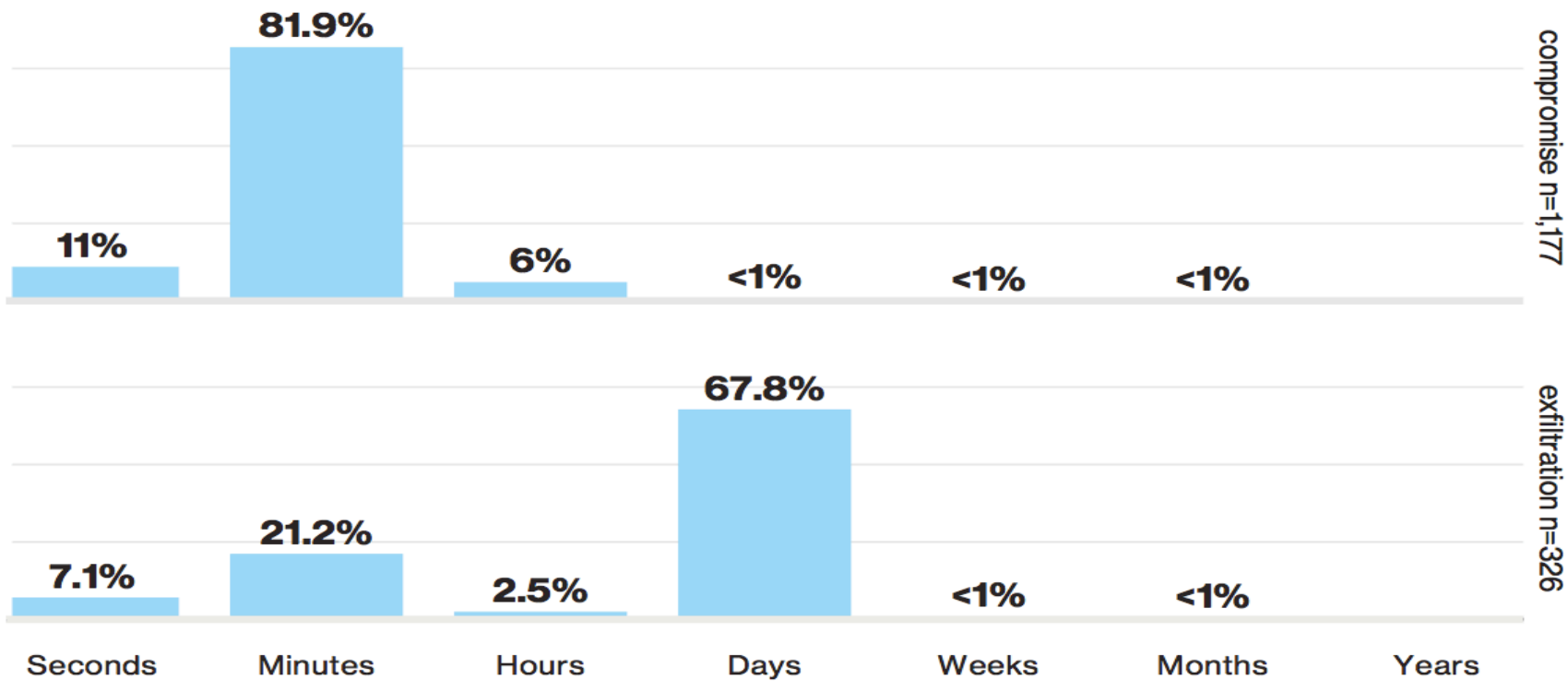


Figure 7
Time to compromise and exfiltration

#8) Intrusion Detection Systems (IDS) are a relatively efficient and effective

Attacks happen fast, Discovering them is usually slow

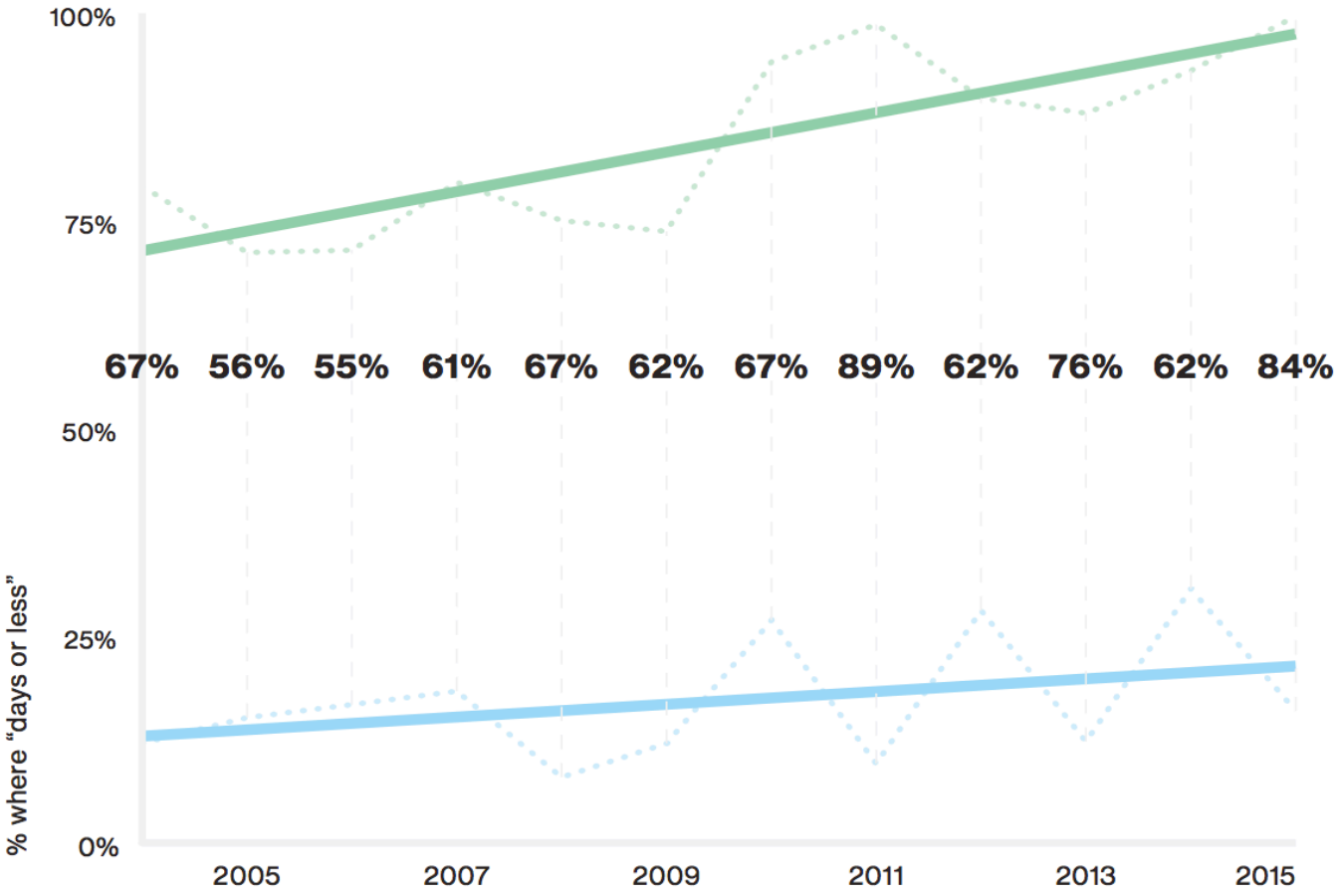


Figure 8.

Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

#8) Intrusion Detection Systems (IDS) are a relatively efficient and effective

Attacks happen fast, Discovering them is usually slow

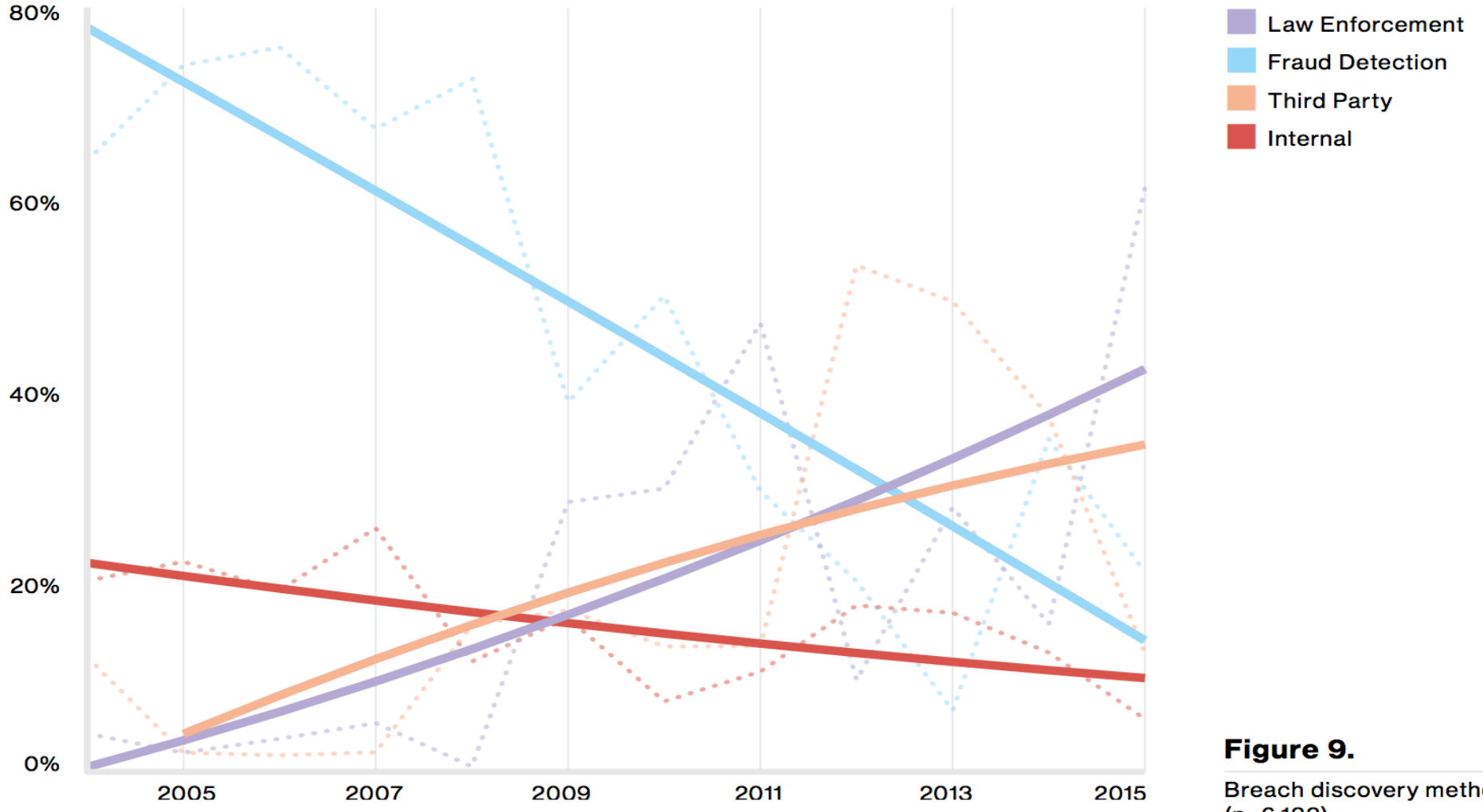


Figure 9.

Breach discovery methods (n=6,133).

#9) Mobile and IoT are the new Big Risks

- ….what isn't in this report. For those looking for proclamations about this being the year that mobile attacks bring us to our knees or that the Internet of Things (IoT) is coming to kill us all, you will be disappointed. We still do not have significant real-world data on these technologies as the vector of attack on organizations.

- Only one possible breach: Code hack, But No confirmed organizations that suffered an attribute loss (therefore no known breaches)

The Nasty Nine:

Turns out None of these are True

1. Risk is most related to vulnerability
2. The best way to reduce risk: implement stronger solutions, policies & training
3. Apply Security Patches Faster for zero day and wildfire increases in risk each time new vulnerabilities are published
4. Encryption data in transit is among top 10 most important controls
   Encryption data at rest is among strongest controls for servers
5. Use Stronger Passwords to reduce risk
6. Use Stronger Identity Proofing to reduce risk
7. HIPAA security standard has a lot of onerous requirements and is among the most complex & difficult to achieve certification
8. Intrusion Detection Systems (IDS) are a relatively efficient and effective
9. Mobile and IoT are the new Big Risks

Summary Actions:

- Use Layers of good standard, basic processes
- Patch 100.0% of everything -- slowly is fine
- Use 2-factor identity for all remote access
- Enable 3rd party security monitoring
- Encrypt Laptops and other portable storage
- Replace FAX & Paper with HIPAA compliant messaging and filtering
- Secure messaging (Strong Identity, logging, encryption, integration) is very resistant to phishing, spam, malicious code, scam and other entry attack vectors.

Nasty Nine Information Security Mistakes

Peter Tippett
Chairman, DataMotion