Evidence Based Risk Management

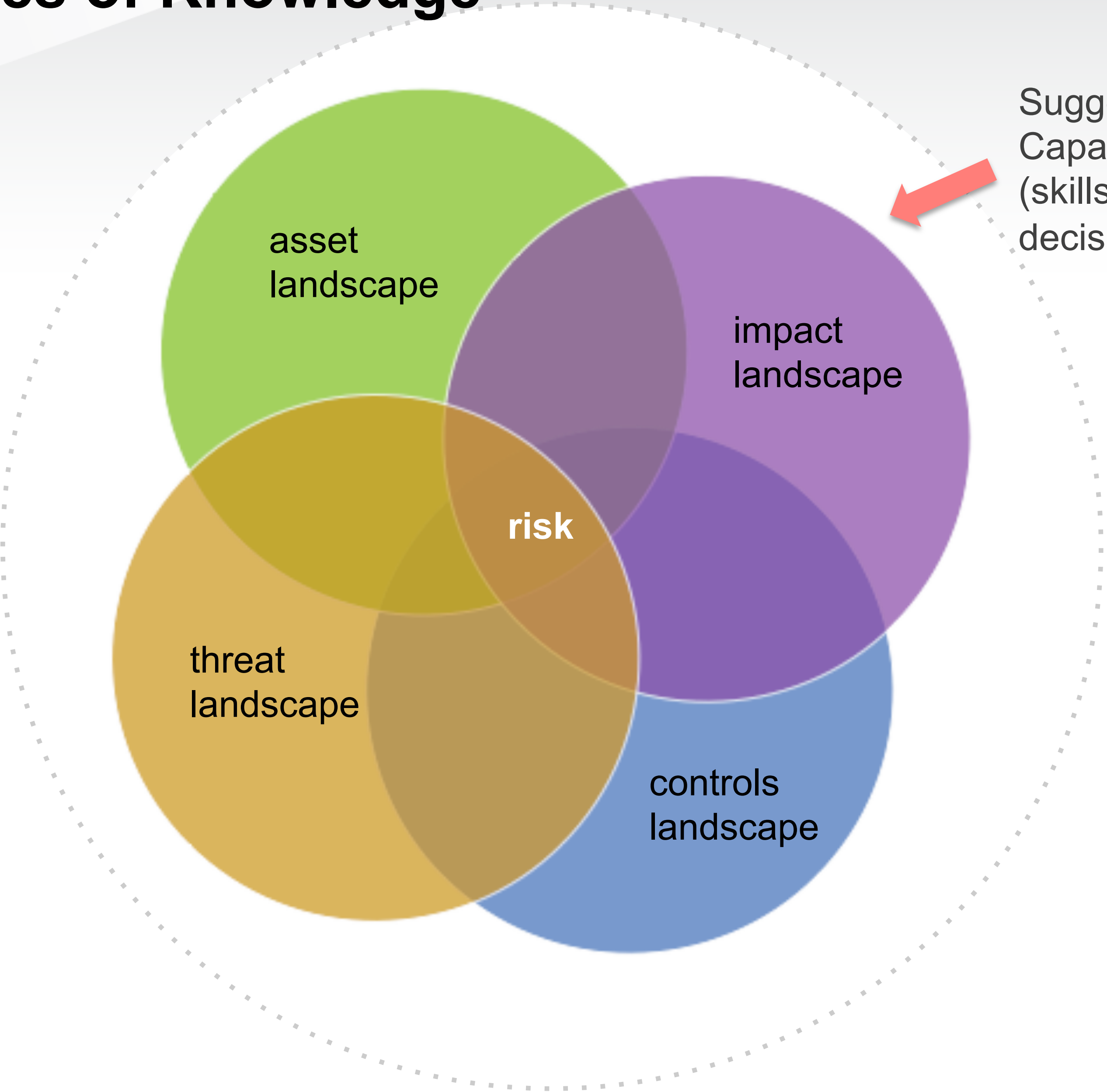
Better management through better measurement

State of the Industry

Pseudoscience or Kuhn’s Protoscience

- somewhat random fact gathering (mainly of readily accessible data)
- a “morass” of interesting, trivial, irrelevant observations
- A variety of theories (that are spawned from what he calls philosophical speculation) that provide little guidance to data gathering

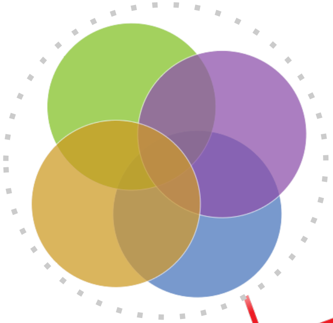
Sources of Knowledge



Suggested context:
Capability to manage
(skills, resources,
decision quality…)

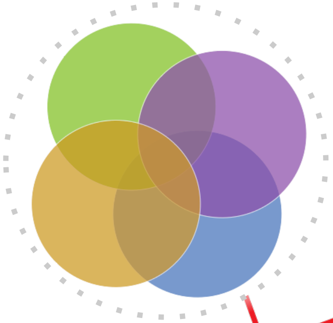
Risk Management

State of Nature	State of Knowledge	State of Wisdom
Evidence level 1	Lists	Feeling like we’ve done something
Evidence level 2	Simple derived values with ad-hoc modeling	Outcomes with ad-hoc deductive selections
Evidence level 3	Formal Modeling	Decision making constructs
Evidence level 4		



Risk Management

State of Nature	State of Knowledge	State of Wisdom
Evidence level 1	Lists	Feeling like we've done something
Evidence level 2	Simple derived values with ad-hoc modeling	Outcomes with ad-hoc deductive selections
Evidence level 3	Formal Modeling	Decision making constructs
Evidence level 4		



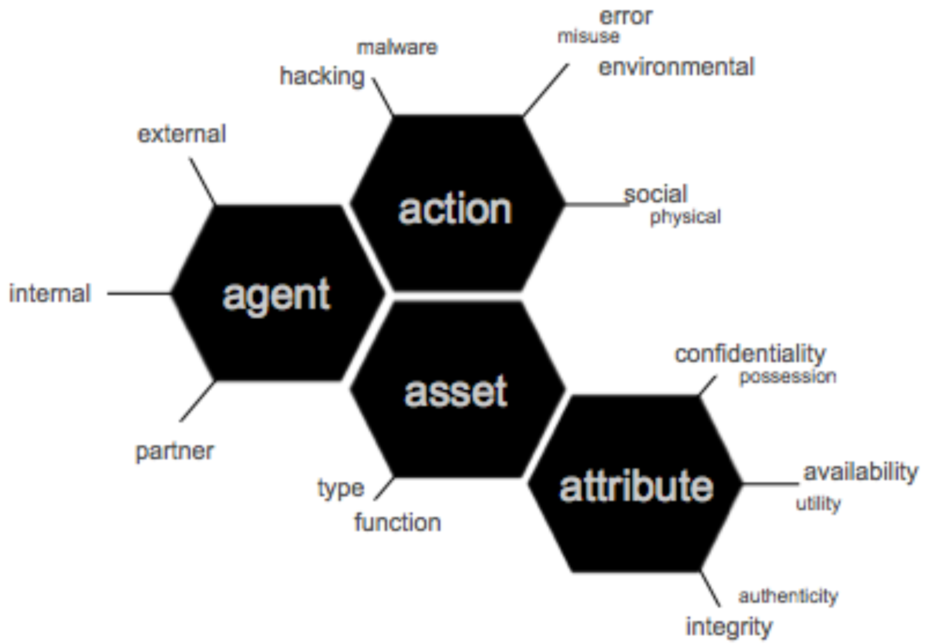
EBRM

State of Nature	State of Knowledge	State of Wisdom
Evidence level 1	Lists	Feeling like we’ve done something
Evidence level 2	Simple derived values with ad-hoc modeling	Outcomes with ad-hoc deductive selections
Evidence level 3	Formal Modeling	Decision making constructs
Evidence level 4		

The VERIS Framework

What is the VERIS framework?

The Incident Classification section employs Verizon's A^4 threat model



A security incident (or threat scenario) is modeled as a series of **events**. Every event is comprised of the following 4 **A**'s:

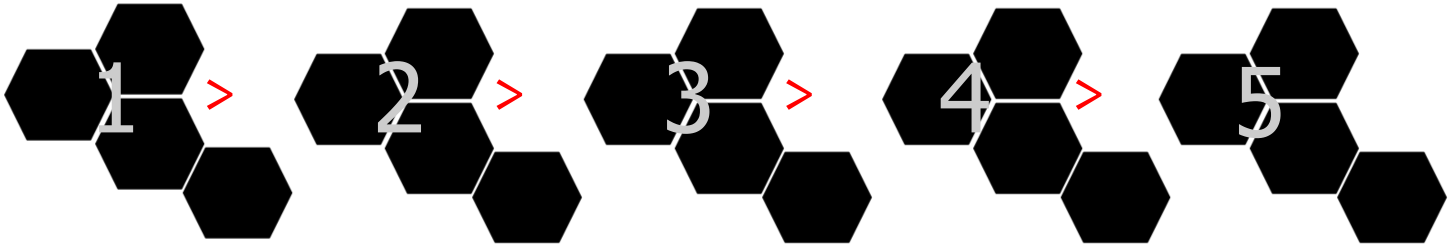
Agent: Whose actions affected the asset

Action: What actions affected the asset

Asset: Which assets were affected

Attribute: How the asset was affected

Incident as a chain of events >



https://verisframework.wiki.zoho.com/

What VERIS does

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

The overall goal is to create a foundation for data-driven decision-making and risk management.

What VERIS does

INCIDENT REPORT

"An attacker from a Russian IP address initiated multiple SQL injection attacks against a public-facing web application. They were able to introduce keyloggers and network sniffers onto internal systems. The keyloggers captured several domain credentials which the attackers used to further infiltrate the corporate network. The packet sniffers captured data for several months which the attacker periodically returned to collect…"

VERIS takes this and…

What VERIS does

Event 1

Agent: External (Org crime)

Action: Hacking (SQLi)

Asset: Server (Web server, Database)

Attribute: Integrity

Event 2

Agent: External (Org crime)

Action: Malware (Keylogger)

Asset: Server (Web server)

Attribute: Confidentiality

Event 3

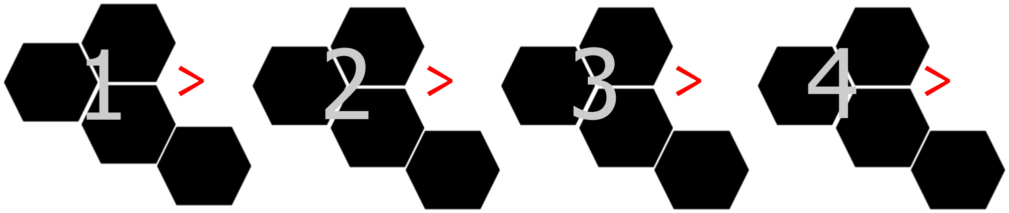
Agent: External (Org crime)

Action: Hacking (Use of stolen creds)

Asset: Server, Network (multiple)

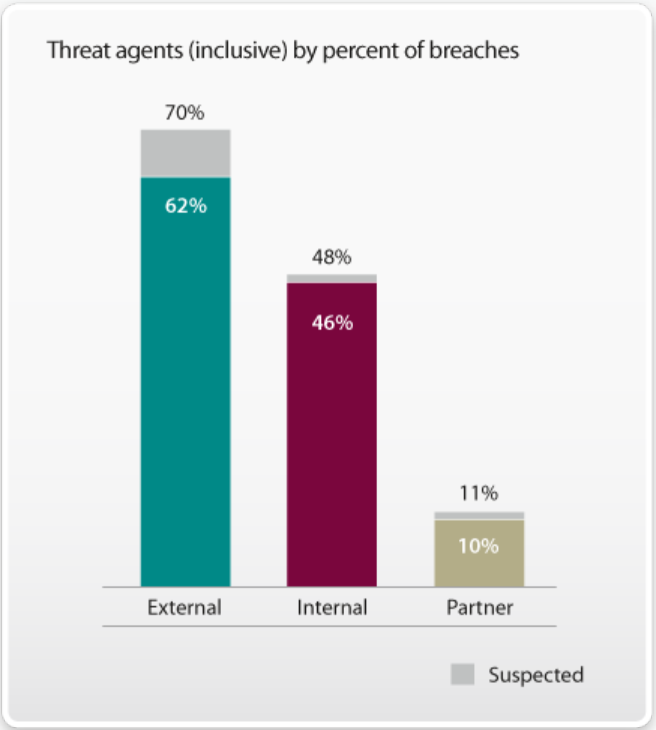
Attribute: Confidentiality, Integrity

Event 4…

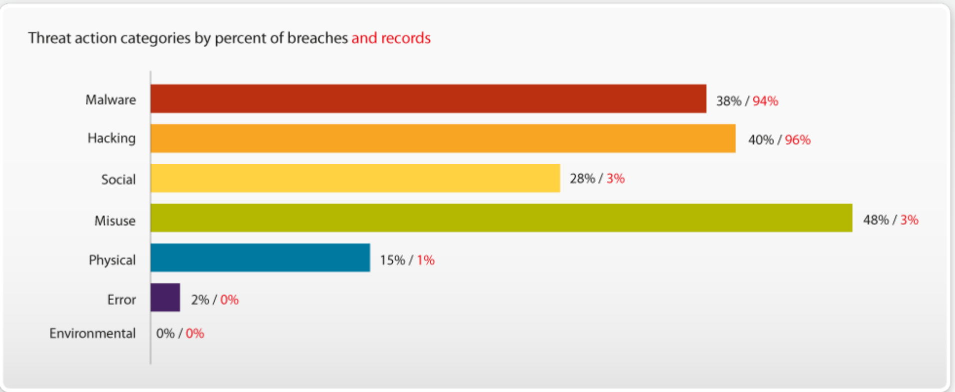


…and translates it to this…

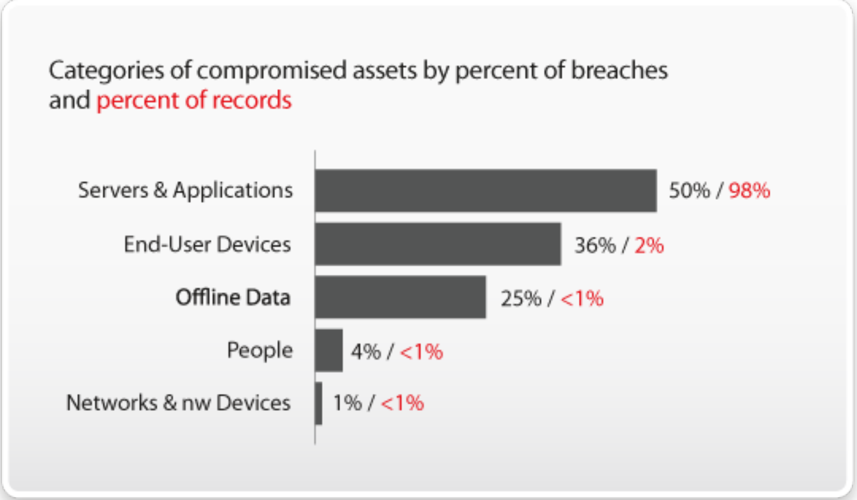
What VERIS does



Threat agents (inclusive) by percent of breaches



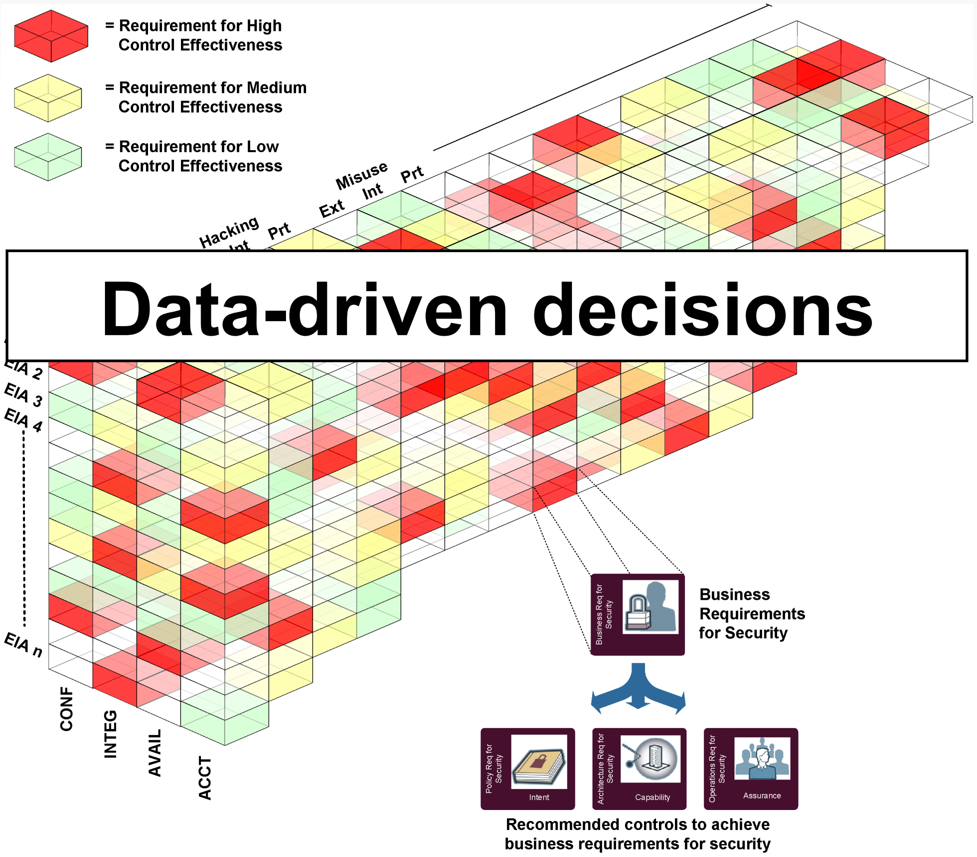
Threat action categories by percent of breaches and records



Categories of compromised assets by percent of breaches and percent of records

…and over time to this…

What VERIS does



🟥 = Requirement for High Control Effectiveness

🟨 = Requirement for Medium Control Effectiveness

🟩 = Requirement for Low Control Effectiveness

Business Requirements for Security

Recommended controls to achieve business requirements for security

Data-driven decisions

…and enables this…

What VERIS does

↓ Risk & ↓ Spending

…to better achieve this.

(and that’s what it’s all about, right?)

The VERIS community project

Community Participation

- 1921 total submissions since launch in November
- Majority resulted from probes and attacks (mostly a bunch of NVPs)
- Many resulted from people playing with the app
- ~ 60 genuine incident submissions

VERIS Community Data

		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
Servers & Apps	Conf	3	2	1	4		1	1	1		1	2	1									
	Poss	5	1		5	1					1			1								
	Integ	5	3		5			2	2		2	2		1								
	Auth	2	1		3	1								1								
	Avail	3	1		5	1	1	1	2	1	2	1	1									
	Util	1	1					1	1		1	1	1									
Networks & Devices	Conf				1						1		1									
	Poss				1						1											
	Integ				2						1			1								
	Auth				1						1											
	Avail				3			1														
	Util																					
End-User Systems	Conf	1		1								1										
	Poss	2	2	1	2	1	1				2	1										
	Integ	3	2	1	2	1	1	1			2	1										
	Auth	1	1								1	1										
	Avail	4	1					2			2	2	1				1	2	1			
	Util																					
Offline Data	Conf												1									
	Poss												1									
	Integ																					
	Auth																					
	Avail												1									
	Util																					
People	Conf							1	1								1	1				
	Poss							1	1													
	Integ							2	1													
	Auth							1	1													
	Avail							1	1													
	Util							1	1													

Let’s look at a scenario

		Ext	Int	Prt	Ext	Int										Prt	Ext	Int	Prt	Ext	Int	Prt
			Malware			Hacking												Physical			Environmental	
Servers & Apps	Conf	3	2	1	4																	
	Poss	5	1		5	1																
	Integ	5	3		5																	
	Auth	2	1		3	1																
	Avail	3	1		5	1																
	Util	1	1																			
Networks & Devices	Conf				1																	
	Poss				1																	
	Integ				2																	
	Auth				1						1											
	Avail				3			1														
	Util																					
End-User Systems	Conf	1		1								1										
	Poss	2	2	1	2	1	1				2	1										
	Integ	3	2	1	2	1	1	1			2	1										
	Auth	1	1								1	1										
	Avail	4	1					2			2	2	1				1	2	1			
	Util																					
Offline Data	Conf												1									
	Poss												1									
	Integ																					
	Auth																					
	Avail												1									
	Util																					
People	Conf							1	1								1	1				
	Poss							1	1													
	Integ							2	1													
	Auth							1	1													
	Avail							1	1													
	Util							1	1													

External
Hacking
Servers & Applications
Confidentiality

2010 Investigative Response Data

		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
Servers & Apps	Conf	45	2	2	63	1	3	3			2	9	1				1					
	Poss	2			2																	
	Integ	48	3	2	50	2	2	4			3	7					1					
	Auth																					
	Avail	4			4																	
	Util																					
Networks & Devices	Conf	2			2			1														
	Poss																					
	Integ	2			2			1														
	Auth																					
	Avail	1			1																	
	Util																					
End-User Systems	Conf	22	3	1	15	1	1	2			3	5					1					
	Poss	2			1																	
	Integ	24	5	1	15	1	1	3	1		4	4					1					
	Auth																					
	Avail	1			1												1					
	Util																					
Offline Data	Conf	1	1								2	3										
	Poss																					
	Integ	1	1								1	1										
	Auth																					
	Avail																					
	Util																					
People	Conf	2			3			2														
	Poss																					
	Integ	2			3			3		1	1		1	1		1						
	Auth																					
	Avail																					
	Util																					

VERIS Community Data

		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
Servers & Apps	Conf	3	2	1	4		1	1	1		1	2	1									
	Poss	5	1		5	1					1			1								
	Integ	5	3		5			2	2		2	2		1								
	Auth	2	1		3	1								1								
	Avail	3	1		5	1	1	1	2	1	2	1	1									
	Util	1	1					1	1		1	1	1									
Networks & Devices	Conf				1						1		1									
	Poss				1						1											
	Integ				2						1			1								
	Auth				1						1											
	Avail				3			1														
	Util																					
End-User Systems	Conf	1		1								1										
	Poss	2	2	1	2	1	1				2	1										
	Integ	3	2	1	2	1	1	1			2	1										
	Auth	1	1								1	1										
	Avail	4	1					2			2	2	1				1	2	1			
	Util																					
Offline Data	Conf												1									
	Poss												1									
	Integ																					
	Auth																					
	Avail												1									
	Util																					
People	Conf							1	1								1	1				
	Poss							1	1													
	Integ							2	1													
	Auth							1	1													
	Avail							1	1													
	Util							1	1													

2010 Investigative Response Data

		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
Servers & Apps	Conf	45	2	2	63	1	3	3			2	9	1				1					
	Poss	2			2																	
	Integ	48	3	2	50	2	2	4			3	7					1					
	Auth																					
	Avail	4			4																	
	Util																					
Networks & Devices	Conf	2			2			1														
	Poss																					
	Integ	2			2			1														
	Auth																					
	Avail	1			1																	
	Util																					
End-User Systems	Conf	22	3	1	15	1	1	2			3	5					1					
	Poss	2			1																	
	Integ	24	5	1	15	1	1	3	1		4	4					1					
	Auth																					
	Avail	1			1												1					
	Util																					
Offline Data	Conf	1	1								2	3										
	Poss																					
	Integ	1	1								1	1										
	Auth																					
	Avail																					
	Util																					
People	Conf	2			3			2														
	Poss																					
	Integ	2			3			3		1	1		1	1		1						
	Auth																					
	Avail																					
	Util																					

verizon

2008-2010 Investigative Response Data

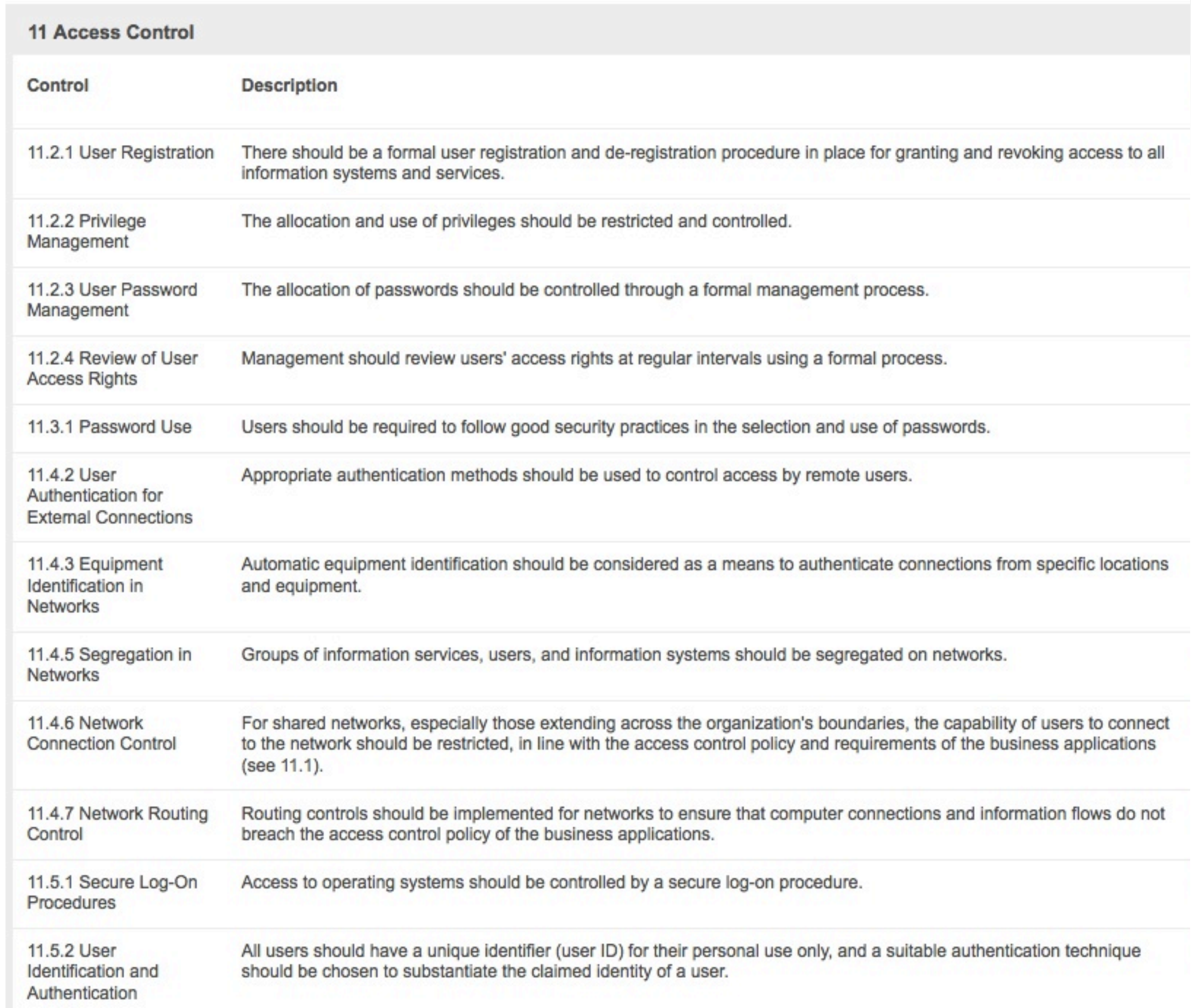
		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
		Malware			Hacking			Social			Misuse			Error			Physical			Environmental		
Servers & Apps	Conf	97	8	18	142	6	31	10	5	2	8	24	7		3		4	5	2			
	Poss	2			2	1		1	2	1	1	3	2				1	3	2			
	Integ	101	9	18	110	5	23	9	4	2	8	15	4				3	2	1			
	Auth				1																	
	Avail	4			4	1		1	2	1	1	3	2				1	3	2			
	Util																					
Networks & Devices	Conf	2			3	1		2	1		1	1										
	Poss																					
	Integ	2			2			1														
	Auth																					
	Avail	1			1																	
	Util																					
End-User Systems	Conf	48	8	5	37	6	9	11	3	1	11	17	4	1	1		6	2	2			
	Poss	2			1			1	1	1	2	2	2	1	1		2	3	2			
	Integ	48	9	6	32	4	6	10	3	2	8	10	4				4	1	2			
	Auth																					
	Avail	1			1			1	1	1	2	2	2	1	1		3	3	2			
	Util																					
Offline Data	Conf	1	1			1			1		2	5	1				1	3	1			
	Poss					1			1			2	1				1	3	1			
	Integ	1	1								1	1										
	Auth																					
	Avail					1			1			2	1				1	3	1			
	Util																					
People	Conf	3	1	1	6	1	1	5	1	1												
	Poss																					
	Integ	3	1	1	4	1	1	4	1	2	1		1	1		1						
	Auth																					
	Avail																					
	Util																					

Let’s look at a scenario

		Ext	Int	Prt	Ext	Int										Prt	Ext	Int	Prt	Ext	Int	Prt
		Malware			Hacking												Physical			Environmental		
Servers & Apps	Conf	3	2	1	4																	
	Poss	5	1		5	1																
	Integ	5	3		5																	
	Auth	2	1		3	1																
	Avail	3	1		5	1																
	Util	1	1																			
Networks & Devices	Conf				1																	
	Poss				1																	
	Integ				2																	
	Auth				1						1											
	Avail				3			1														
	Util																					
End-User Systems	Conf	1		1								1										
	Poss	2	2	1	2	1	1				2	1										
	Integ	3	2	1	2	1	1	1			2	1										
	Auth	1	1								1	1										
	Avail	4	1					2			2	2	1				1	2	1			
	Util																					
Offline Data	Conf												1									
	Poss												1									
	Integ																					
	Auth																					
	Avail												1									
	Util																					
People	Conf							1	1								1	1				
	Poss							1	1													
	Integ							2	1													
	Auth							1	1													
	Avail							1	1													
	Util							1	1													

External
Hacking
Servers & Applications
Confidentiality

What controls would be relevant to this scenario?



11 Access Control

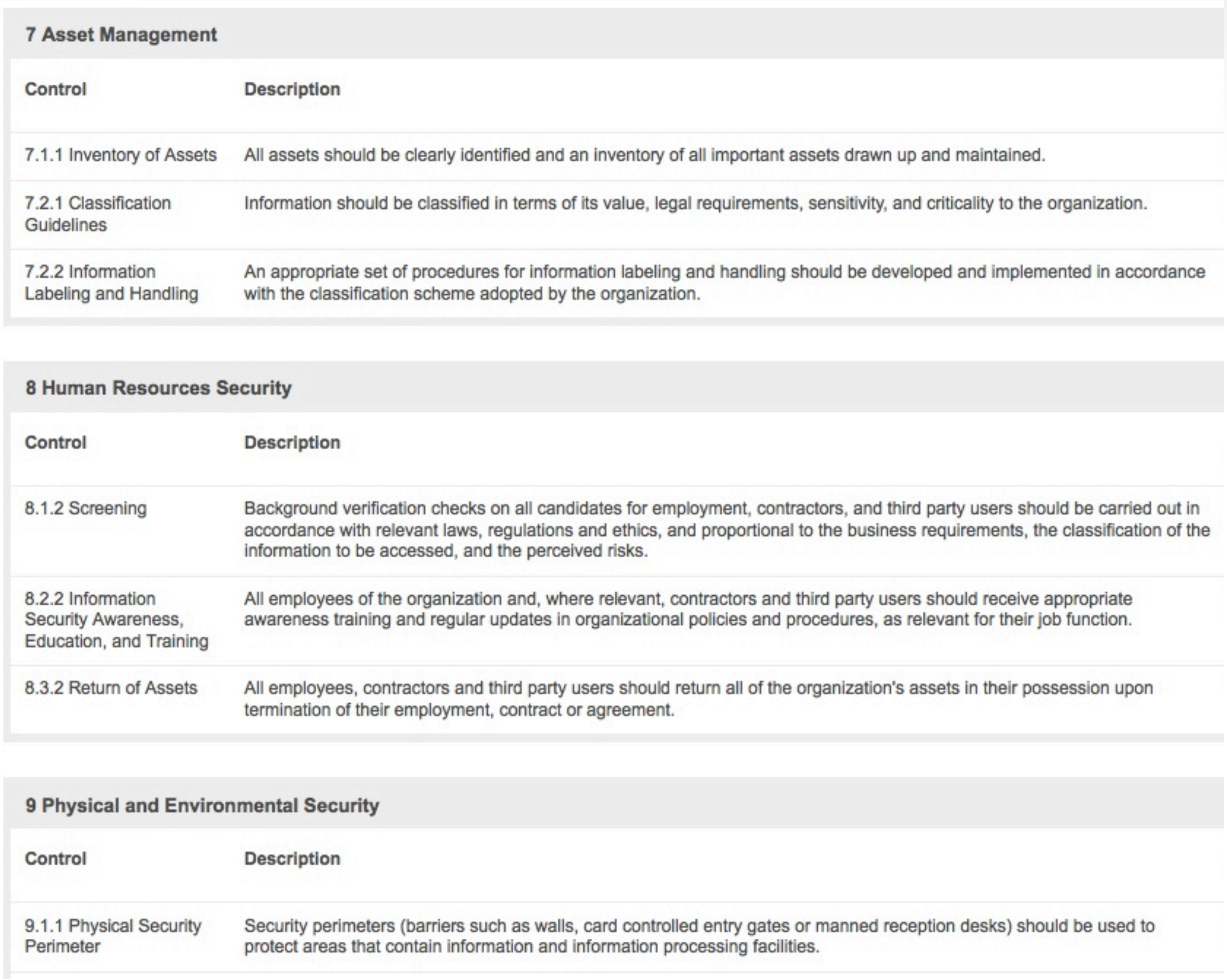
Control	Description
11.2.1 User Registration	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
11.2.2 Privilege Management	The allocation and use of privileges should be restricted and controlled.
11.2.3 User Password Management	The allocation of passwords should be controlled through a formal management process.
11.2.4 Review of User Access Rights	Management should review users' access rights at regular intervals using a formal process.
11.3.1 Password Use	Users should be required to follow good security practices in the selection and use of passwords.
11.4.2 User Authentication for External Connections	Appropriate authentication methods should be used to control access by remote users.
11.4.3 Equipment Identification in Networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
11.4.5 Segregation in Networks	Groups of information services, users, and information systems should be segregated on networks.
11.4.6 Network Connection Control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).
11.4.7 Network Routing Control	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
11.5.1 Secure Log-On Procedures	Access to operating systems should be controlled by a secure log-on procedure.
11.5.2 User Identification and Authentication	All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

How about another scenario?

		Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt	Ext	Int	Prt
			Malware			Hacking			Social			Misuse			Error			Physical			Environmental	
Servers & Apps	Conf	97	8	18	142	6	31	10	5	2	8	24	7		3		4	5	2			
	Poss	2			2	1		1	2	1	1	3	2				1	3	2			
	Integ	101	9	18	110	5	23	9	4	2	8	15	4				3	2	1			
	Auth				1																	
	Avail	4			4	1		1	2	1	1	3	2				1	3	2			
	Util																					
Networks & Devices	Conf	2			3	1		2	1		1	1										
	Poss																					
	Integ	2			2			1														
	Auth																					
	Avail	1			1																	
	Util																					
End-User Systems	Conf	48	8	5	37	6	[illegible]								[illegible]		6	2	2			
	Poss	2			1										[illegible]		2	3	2			
	Integ	48	9	6	32	4	[illegible]								[illegible]		4	1	2			
	Auth																					
	Avail	1			1										[illegible]		3	3	2			
	Util																					
Offline Data	Conf	1	1			1											1	3	1			
	Poss					1											1	3	1			
	Integ	1	1																			
	Auth																					
	Avail					1			1			2	1				1	3	1			
	Util																					
People	Conf	3	1	1	6	1	1	5	1	1												
	Poss																					
	Integ	3	1	1	4	1	1	4	1	2	1		1	1		1						
	Auth																					
	Avail																					
	Util																					

External
Physical
Offline Data
Confidentiality

What controls would be relevant to this scenario?



7 Asset Management

Control	Description
7.1.1 Inventory of Assets	All assets should be clearly identified and an inventory of all important assets drawn up and maintained.
7.2.1 Classification Guidelines	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
7.2.2 Information Labeling and Handling	An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.

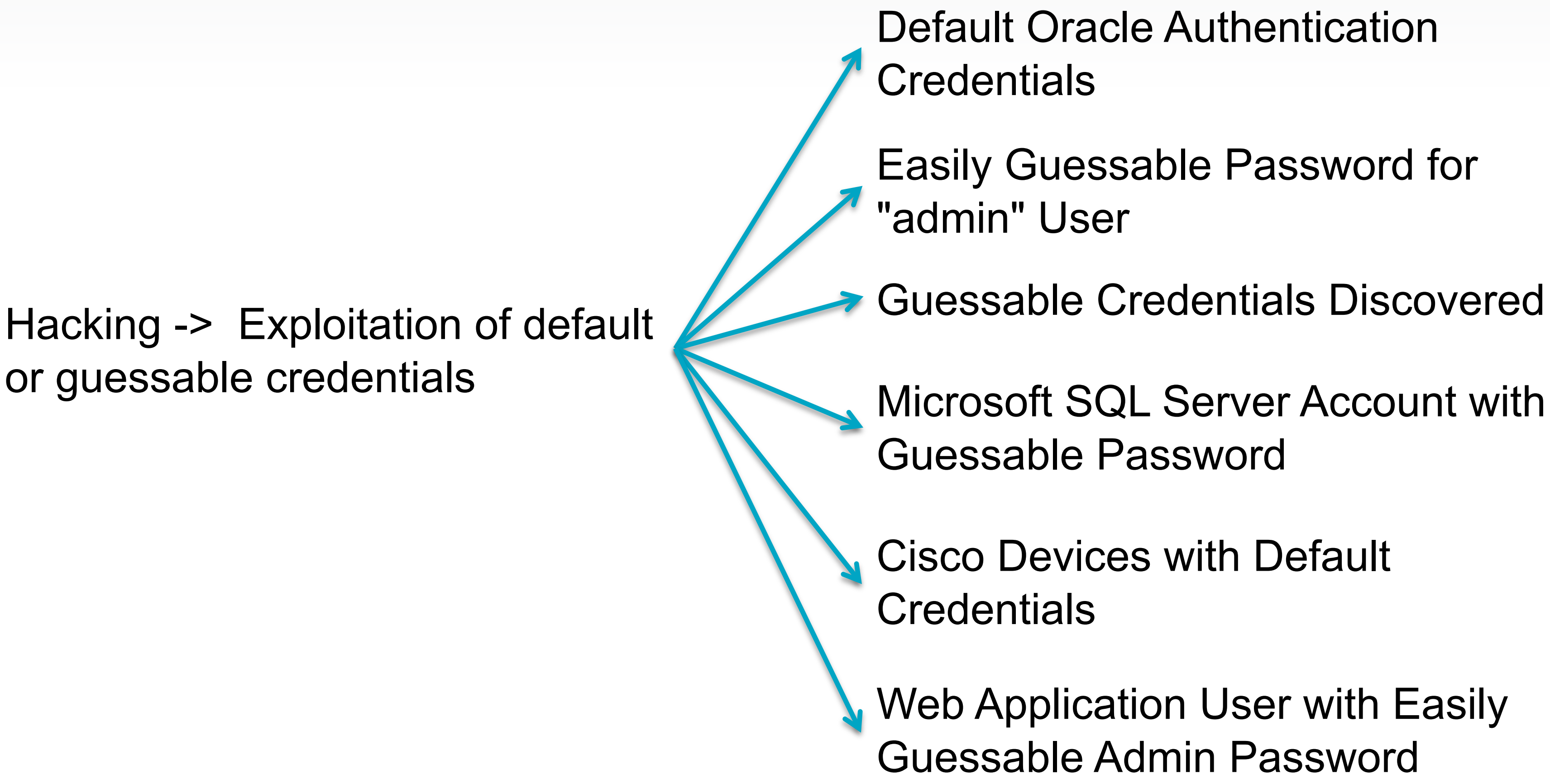
8 Human Resources Security

Control	Description
8.1.2 Screening	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
8.2.2 Information Security Awareness, Education, and Training	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
8.3.2 Return of Assets	All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

9 Physical and Environmental Security

Control	Description
9.1.1 Physical Security Perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Mapping action types to identified vulnerabilities



Hacking -> Exploitation of default or guessable credentials

Default Oracle Authentication Credentials

Easily Guessable Password for "admin" User

Guessable Credentials Discovered

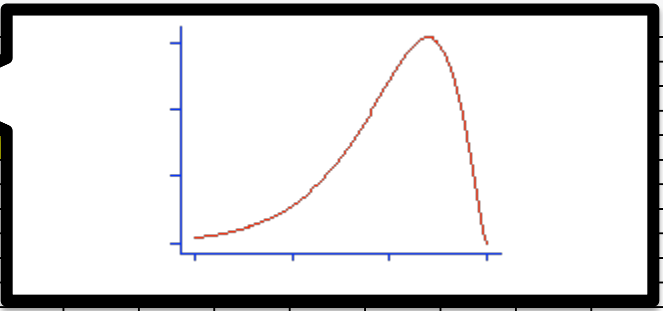
Microsoft SQL Server Account with Guessable Password

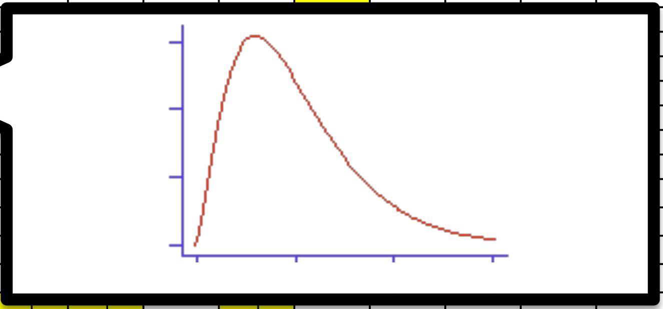
Cisco Devices with Default Credentials

Web Application User with Easily Guessable Admin Password

Measure distributions of impact

		Ext	Int	Prt	Ext	Int										Prt	Ext	Int	Prt	Ext	Int	Prt
			Malware			Hacking												Physical			Environmental	
Servers & Apps	Conf	45	2	2	63	[illegible]											1					
	Poss	2			2																	
	Integ	48	3	2	[illegible]	2	[illegible]										1					
	Auth																					
	Avail	4			4																	
	Util																					
Networks & Devices	Conf	2			2																	
	Poss																					
	Integ	2			2																	
	Auth																					
	Avail	1			1																	
	Util																					
End-User Systems	Conf	22	3	1	15	1	1	2			3	5					1					
	Poss	2			1																	
	Integ	24	5	1	15	1	1	3	1		4	4					1					
	Auth																					
	Avail	1			1																	
	Util																					
Offline Data	Conf	1	1								2											
	Poss																					
	Integ	1	1								1	1										
	Auth																					
	Avail																					
	Util																					
People	Conf	2			3			2														
	Poss																					
	Integ	2			3			3		1	1		[illegible]	[illegible]		[illegible]						
	Auth																					
	Avail																					
	Util																					

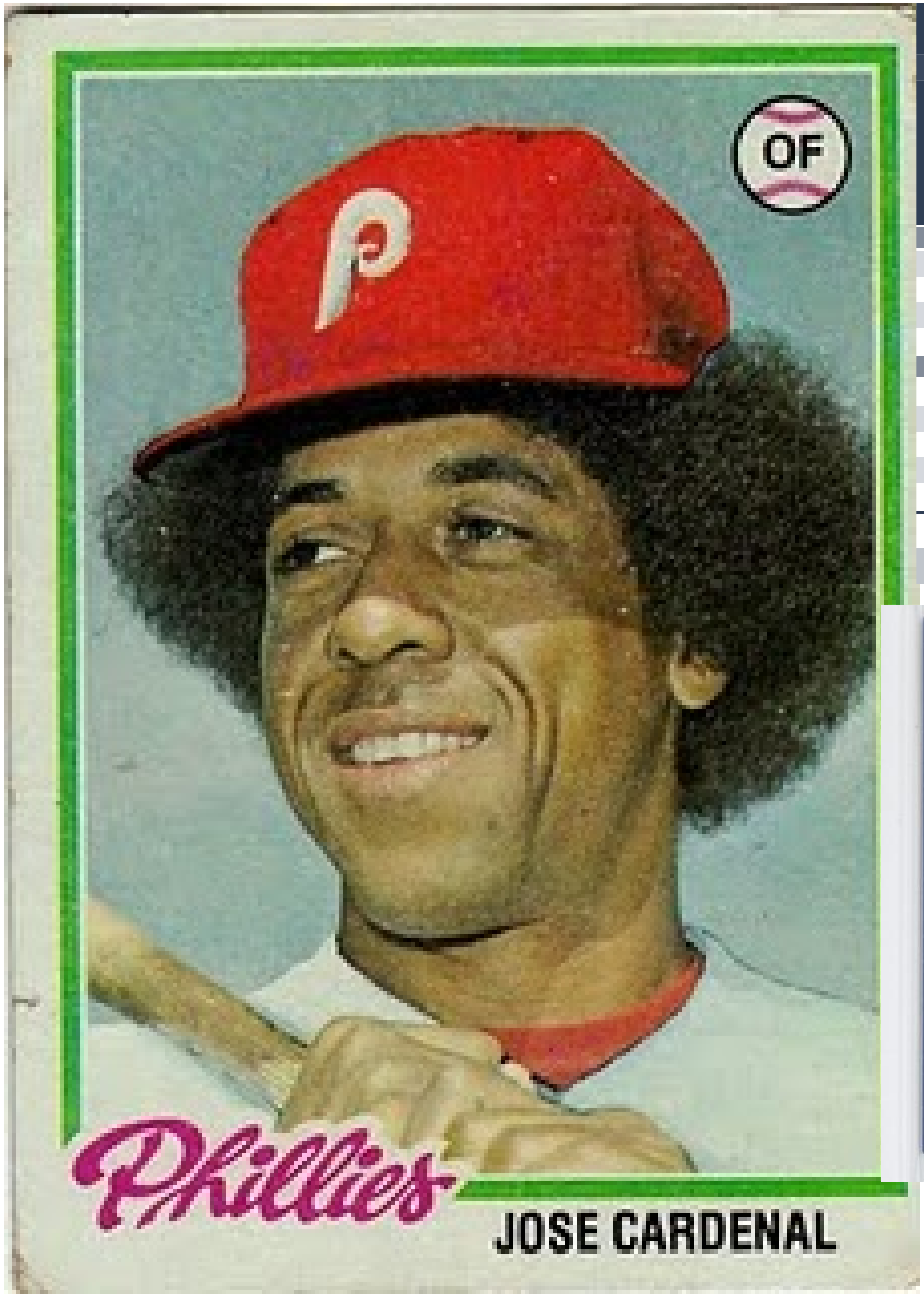


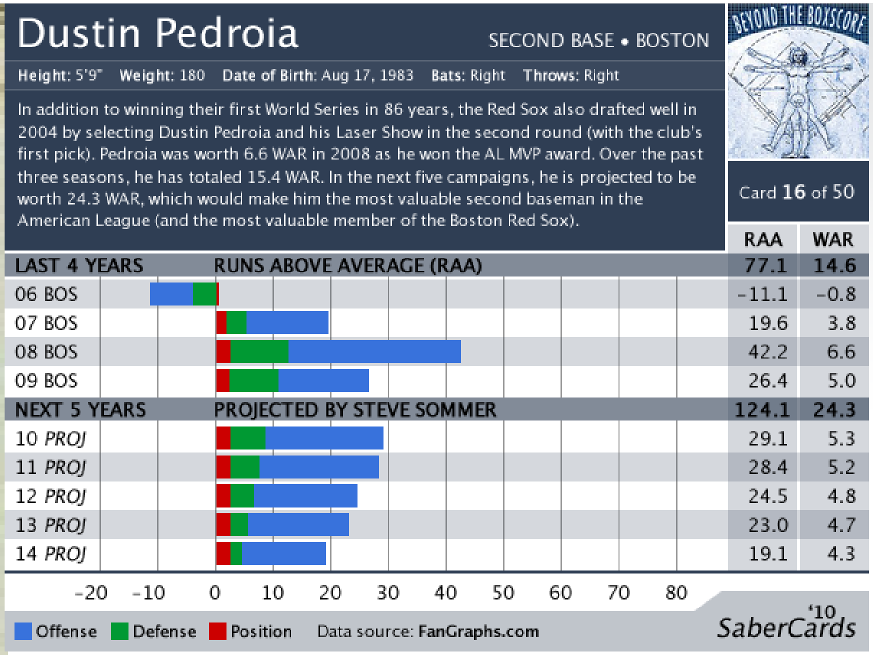


So…where can we head with all this?

- Understand control effectiveness
- Identify control efficiencies
- Identify optimized controls sets

A vision of EBRM Metrics





Dustin Pedroia

SECOND BASE • BOSTON

Height: 5'9" **Weight:** 180 **Date of Birth:** Aug 17, 1983 **Bats:** Right **Throws:** Right

In addition to winning their first World Series in 86 years, the Red Sox also drafted well in 2004 by selecting Dustin Pedroia and his Laser Show in the second round (with the club's first pick). Pedroia was worth 6.6 WAR in 2008 as he won the AL MVP award. Over the past three seasons, he has totaled 15.4 WAR. In the next five campaigns, he is projected to be worth 24.3 WAR, which would make him the most valuable second baseman in the American League (and the most valuable member of the Boston Red Sox).

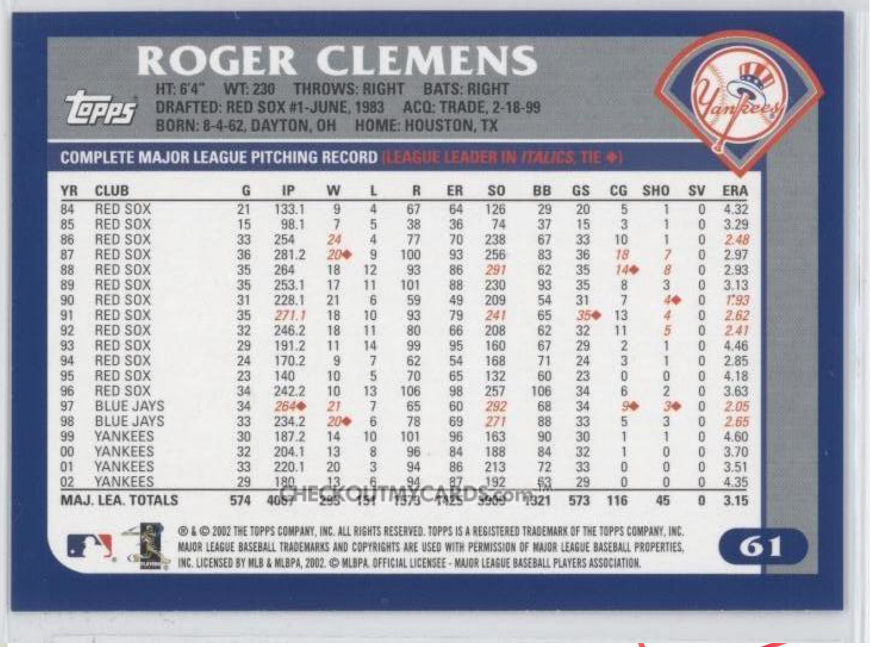
BEYOND THE BOXSCORE

Card **16** of 50

LAST 4 YEARS	RUNS ABOVE AVERAGE (RAA)	RAA	WAR
		77.1	14.6
06 BOS		-11.1	-0.8
07 BOS		19.6	3.8
08 BOS		42.2	6.6
09 BOS		26.4	5.0
NEXT 5 YEARS	**PROJECTED BY STEVE SOMMER**	124.1	24.3
10 *PROJ*		29.1	5.3
11 *PROJ*		28.4	5.2
12 *PROJ*		24.5	4.8
13 *PROJ*		23.0	4.7
14 *PROJ*		19.1	4.3

🟦 Offense 🟩 Defense 🟥 Position Data source: **FanGraphs.com**

'10 SaberCards



ROGER CLEMENS

HT: 6'4" WT: 230 THROWS: RIGHT BATS: RIGHT
DRAFTED: RED SOX #1-JUNE, 1983 ACQ: TRADE, 2-18-99
BORN: 8-4-62, DAYTON, OH HOME: HOUSTON, TX

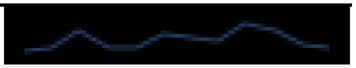
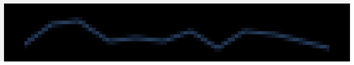
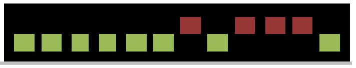
Topps
Yankees

COMPLETE MAJOR LEAGUE PITCHING RECORD (LEAGUE LEADER IN *ITALICS*, TIE ◆)

YR	CLUB	G	IP	W	L	R	ER	SO	BB	GS	CG	SHO	SV	ERA
84	RED SOX	21	133.1	9	4	67	64	126	29	20	5	1	0	4.32
85	RED SOX	15	98.1	7	5	38	36	74	37	15	3	1	0	3.29
86	RED SOX	33	254	*24*	4	77	70	238	67	33	10	1	0	*2.48*
87	RED SOX	36	281.2	*20*◆	9	100	93	256	83	36	*18*	*7*	0	2.97
88	RED SOX	35	264	18	12	93	86	*291*	62	35	*14*◆	*8*	0	2.93
89	RED SOX	35	253.1	17	11	101	88	230	93	35	8	3	0	3.13
90	RED SOX	31	228.1	21	6	59	49	209	54	31	7	*4*◆	0	*1.93*
91	RED SOX	35	*271.1*	18	10	93	79	*241*	65	*35*◆	13	*4*	0	*2.62*
92	RED SOX	32	246.2	18	11	80	66	208	62	32	11	*5*	0	*2.41*
93	RED SOX	29	191.2	11	14	99	95	160	67	29	2	1	0	4.46
94	RED SOX	24	170.2	9	7	62	54	168	71	24	3	1	0	2.85
95	RED SOX	23	140	10	5	70	65	132	60	23	0	0	0	4.18
96	RED SOX	34	242.2	10	13	106	98	257	106	34	6	2	0	3.63
97	BLUE JAYS	34	*264*◆	*21*	7	65	60	*292*	68	34	*9*◆	*3*◆	0	*2.05*
98	BLUE JAYS	33	234.2	*20*◆	6	78	69	*271*	88	33	5	3	0	*2.65*
99	YANKEES	30	187.2	14	10	101	96	163	90	30	1	1	0	4.60
00	YANKEES	32	204.1	13	8	96	84	188	84	32	1	0	0	3.70
01	YANKEES	33	220.1	20	3	94	86	213	72	33	0	0	0	3.51
02	YANKEES	29	180	13	6	94	87	192	63	29	0	0	0	4.35
MAJ. LEA. TOTALS		574	4067	293	151	1573	1425	3909	1321	573	116	45	0	3.15

61

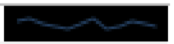
Incident Frequency – Executive Dashboard

frequency of incidents		this month	last month		Quarter Ave	month vs. quarter (ave.)	Annual Ave	month vs. year (ave.)	
	XYZ abc	7	1	⬆	5.7	⬆	7.8	-9.7%	
	peer group	9	5	⬆	2.7	⬆	8.2	10.2%	
	XYZabc vs Peers	-2	-4		3		-0.42	⬇	

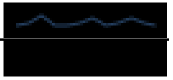
Agent Breakdown (High Level)

Agent (External/Internal/Partner)		this month	last month		Quarter Ave	month vs. quarter (ave.)	Annual Ave	month vs. year (ave.)	
XYZabc	External Agents	6	1	⬆	3.7	⬆	4.3	38.5%	
	Internal Agents	1	0	⬆	1.7	⬇	2.8	-63.6%	
	Partner Agents	2	0	⬆	0.3	⬆	0.7	200.0%	
	Total	9	1		5.7	59%	7.8	16.1%	
peer group (average)	External Agents	6	5	⬆	3.7	62%	1.0	500.0%	
	Internal Agents	2	3	⬇	1.7	18%	14.0	-85.7%	
	Partner Agents	1	1	▭	0.3	233%	2.0	-50.0%	
	Total	9	9		5.7	58%	17.0	-47.1%	
XYZabc vs. Peer		-1	-8		0.0		-9.3		

Action Breakdown (High Level)

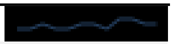
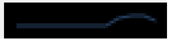
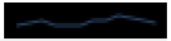
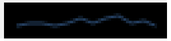
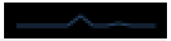
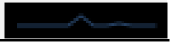
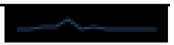
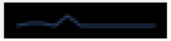
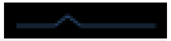
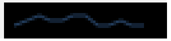
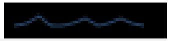
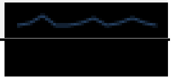
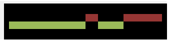
Actions		this month	last month		Quarter Ave	month vs. quarter (ave.)	Annual Ave	month vs. year (ave.)	
XYZabc	Hacking	3	1	⬆	1.7	⬆	2.0	50.0%	
	Malware	2	1	⬆	3.0	⬇	3.7	-45.5%	
	Social	2	0	⬆	1.0	⬆	1.3	50.0%	
	Misuse	0	0	--	2.0	⬇	1.8	-100.0%	
	Physical	0	0	--	0.0	--	0.1	-100.0%	
	Error	0	0	--	0.3	⬇	1.8	-100.0%	
	Environmental	0	0	--	0.0	--	0.3	-100.0%	
	Total	**7**	**2**		**8.0**		**10.8**	-35.4%	
peer group	Hacking	4	5	⬇	4.0	--	2.9	37.1%	
	Malware	6	8	⬇	7.0	⬇	4.7	28.6%	
	Social	2	3	⬇	3.0	⬇	2.5	-20.0%	
	Misuse	4	5	⬇	6.0	⬇	3.3	20.0%	
	Physical	0	0	--	0.0	--	0.8	-100.0%	
	Error	2	3	⬇	1.3	⬆	1.3	50.0%	
	Environmental	1	1	--	0.0	--	1.4	-29.4%	
	Total	19	25	-24%	21.3		17.0	11.8%	
XYZabc vs. Peer		-26	-23		-13.3		-6.2		

Asset Breakdown (High Level)

Assets		**this month**	last month	month over month change	Quarter Ave	month vs. quarter (ave.)	12 month running average	month vs. 12 month (ave.)	
XYZabc	Servers & Applications	3	1	↑	2.7	↑	3.8	-20%	
	Networks & network devices	2	1	↑	1.7	↑	2.1	-4%	
	End User devices	1	0	↑	1.0	--	2.0	-50%	
	Offline data	0	0	--	0.7	--	0.7	-100%	
	People	2	0	↑	1.0	↑	0.8	140%	
		8	2		7.0	14%	9.3	-14%	
peer group	Servers & Applications	8	4	↑	6.7	↑	10.2	-21%	
	Networks & network devices	2	2	--	3.0	↓	2.7	-25%	
	End User devices	9	5	↑	5.7	↑	27.8	-68%	
	Offline data	0	0	--	1.0	--	0.8	-100%	
	People	1	1	--	2.3	--	1.9	-48%	
		20	12		18.7	7%	43.4	-54%	
XYZabc vs. Peer		-12	-10		-11.7		-34.1	-64.8%	

verizon

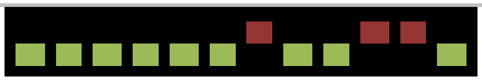
Attribute Breakdown (High Level)

Attributes		this month	last month	month over month change	Quarter Ave	month vs. quarter (ave.)	12 month running ave.	month vs. 12 mos.	
XYZabc	Confidentiality	3	1	↑	1.7	↑	2.9	3%	
	Control	0	0	--	0.7	↓	2.0	-100%	
	Integrity	2	1	↑	2.0	--	2.7	-25%	
	Authenticity	0	0	--	0.7	↓	1.4	-100%	
	Availability	2	0	↑	1.0	↑	2.2	-8%	
	Utility	0	0	--	0.7	↓	1.7	-100%	
		7	2		6.7		12.8		
peer group	Confidentiality	3	4	↓	4.7	↓	4.1	-27%	
	Control	1	4	↓	4.7	↓	2.8	-65%	
	Integrity	3	3	--	4.3	↓	3.1	-3%	
	Authenticity	1	3	↓	3.3	↓	2.8	-64%	
	Availability	2	0	↑	1.3	↑	2.1	-4%	
	Utility	1	0	↑	0.7	↑	1.5	-33%	
		11	14		19.0		16.3		
XYZabc vs. Peer		-4	-12		-12.3		-3.5		

Incident Impact – Executive Dashboard

		estimated (this month)		estimated (ytd)		ytd actual
impact of incidents		min	max	min	max	
	XYZabc	$25,000	$85,000	$300,000	$750,000	$423,000
	Peer (average)	$43,000	$70,000	$508,000	$1,200,000	$578,000

impact performance



12 month "win/loss" (XYZabc vs. Peer average)

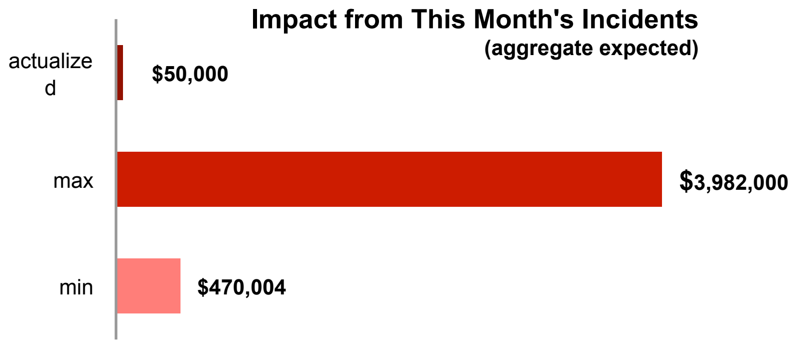
(red indicates months where XYZabc exceeded Peer)

estimation accuracy (estimated vs. actual)

under	within range	over
15%	28%	57%

Impact (High Level)

impact of incidents	estimated (this month) min	 max	estimated (ytd) min	 max	ytd actual
XYZabc	**$470,004**	**$3,982,000**	**$3,290,028**	**$64,587,000**	**$2,303,020**
Productivity	$120,001	$401,000	$840,007	$6,015,000	$588,004.90
Response	$80,002	$181,000	$560,014	$2,172,000	$392,009.80
CA	$0	$0	$98,701	$40,000,000	$0
Brand & Market	$20,000	$2,000,000	$140,000	$2,000,000	$98,000
Operational	$150,000	$300,000	$987,008	$1,200,000	$735,000
Legal & Reg	$100,001	$1,100,000	$658,006	$13,200,000	$490,004.90
Peer (average)	**$611,005**	**$3,185,600**	**$3,454,529**	**$103,339,200**	**$3,224,227**


Impact from This Month's Incidents
(aggregate expected)

Incident Impact –Impact Values By High Level Determinants

		estimated (this month)		estimated (ytd)		ytd actual
impact of incidents		min	max	min	max	
	XYZabc	**$470,004**	**$3,982,000**	**$3,290,028**	**$64,587,000**	**$2,303,020**
Agents	**External Agents**	$120,001	$401,000	$840,007	$6,015,000	$588,004.90
	Internal Agents	$80,002	$181,000	$560,014	$2,172,000	$392,009.80
	Partner Agents	$0	$0	$98,701	$40,000,000	$0
Actions	**Hacking**	$164,501.40	$1,393,700.00	$1,118,610	$21,959,580	$783,027
	Malware	$183,301.56	$1,552,980.00	$1,283,111	$25,188,930	$898,178
	Social	$134,286.86	$1,137,714.29	$460,604	$9,042,180	$322,423
	Misuse	$0	$0	$756,706	$14,855,010	$529,695
	Physical	$0	$0	$39,480	$775,044	$27,636
	Error	$0	$0	$263,202	$5,166,960	$184,242
	Environmental	$0	$0	$55,930	$1,097,979	$39,151
Assets	**Servers & Applications**	$176,251.50	$1,493,250	$1,321,886.25	$25,950,133.93	$925,320.54
	Networks & network devices	$117,501	$995,500	$734,381.25	$14,416,741.07	$514,066.96
	End User devices	$58,750.50	$497,750	$705,006	$13,840,071.43	$493,504.29
	Offline data	$0	$0	$235,002	$4,613,357.14	$164,501.43
	People	$117,501	$995,500	$293,752.50	$5,766,696.43	$205,626.79

Determinant Drill-Down

	Worst Agents	Worst Actions	Worst Assets
Determinants	External, Organized Crime Eastern Europe	Hacking, SQLi	Servers& Applications: Web Server
Mean Losses	$616,950	$385,952	$702,000
Determinants	Internal, Auditors	Misuse, Embezzlement, skimming, and related fraud	Servers& Applications: Remote Acces Server
Mean Losses	$472,000	$287,000	$583,000
Determinants	External, Organized Crime Unknown	Social, Phishing	End User devices Laptoop
Mean Losses	$247,000	$125,000	$297,000
Determinants	Partner, Data storage / archiving	Physical, Theft	People Auditors
Mean Losses	$95,000	$121,000	$178,000

DBIR: www.verizonbusiness.com/databreach
VERIS: https://verisframework.wiki.zoho.com/
Blog: securityblog.verizonbusiness.com
Email: dbir@verizonbusiness.com