



ISSA

Information Systems Security Association
International

www.issa.org

ISSA International Webinar

Key & Residual Risk Indicators

Tuesday, October 23rd, 2018



Moderator

Matt Mosley, Vice President Security Products, Devo

Matt Mosley is the Vice President of Security Products for Devo, a leading SIEM and big data analytics vendor. Matt is a recognized security expert and thought leader with more than 25 years of experience in numerous roles as a practitioner, consultant and software executive. Prior to joining Devo, Matt was the Director of Product Management for Symantec's MSSP business, where he helped to launch new products and services to enhance the security of some of the world's largest organizations. Matt has also held senior leadership roles with leading security firms including NetIQ, Internet Security Systems, Intellitactics, and Brabeion Software.

As the chief security officer at early Internet pioneer DIGEX, Matt defined and implemented the security controls and best practices for the world's first web hosting business and was a founding member of the ISP Security Consortium. Matt holds the CISSP, CISM, and CISA designations, is a regular speaker at security conferences, and taught CISSP classes for ISSA-NOVA for nearly a decade.

Key & Residual Risk Indicators



Speaker

Pete Lindstrom Research Vice President, Security Strategies

Pete Lindstrom is Research Vice President for Security Strategies. His research is focused on digital security measurement and metrics, digital security economics, and digital security at scale. Mr. Lindstrom is responsible for driving the vision of enabling digital transformation through proper technology risk management that makes efficient and effective economic decisions supported by evidence and outcome analysis leading to a security model that aligns with the 3d platform.

Prior to joining IDC in 2014, Mr. Lindstrom accumulated 25 years of industry experience as an IT auditor, IT security practitioner, and industry analyst. He has extensive and broad expertise with a variety of information security products, but is best known as an authority on cybersecurity economics issues, such as strategic security metrics, estimating risk and return, and measuring security programs. He has also focused on applying core risk management principles to new technologies, architectures, and systems, focusing on the use of virtualization, cloud security, and big data. He has developed the "Four Disciplines of Security Management" (a security operations model), and the "5 Immutable Laws of Virtualization Security," which was integrated into guidance from the PCI Council.

Mr. Lindstrom is a frequent contributor to popular business and trade publications. He is often quoted in USA Today, WSJ Online, Information Security Magazine, VAR Business, Searchsecurity.com, and CSO Magazine. His columns and articles have appeared in Information Security Magazine, Searchsecurity.com, ISSA Journal, and CSO Online. Additionally, Mr. Lindstrom is a popular speaker at the RSA Security Conference, InfoSec World, ISSA International Conference, and many regional conferences.

In addition, to his extensive industry experience, Mr. Lindstrom served as an officer in the U.S. Marine Corps and received a bachelor's degree in Business Administration (Finance) from the University of Notre Dame.



Speaker

Michael F. Angelo, CRISC, CISSP

Michael F. Angelo CRISC, CISSP has over 30 years of information assurance experience. Michael has served as a trusted security advisor and security architect with leading corporations and government entities. He has acted as a technical adviser in the development of US national and international export controls. Currently chairs the ISSA International Webinar committee. Amongst his accomplishments he is an ISSA Fellow, and is named on the ISSA Hall of FAME for his contributions to the security community. In addition, he currently holds 61 US Granted Patents. His current work encompasses certifications, SDL, Threat Modeling, AppSec / DevOPS, as well as and Software Supply Chain analysis. Michael is a veteran moderator and has appeared at numerous International conference and in a multitude of International Web Conferences.



Key Risk Indicators for Digital Security

Pete Lindstrom
VP, Security Strategies
IT Executive Program

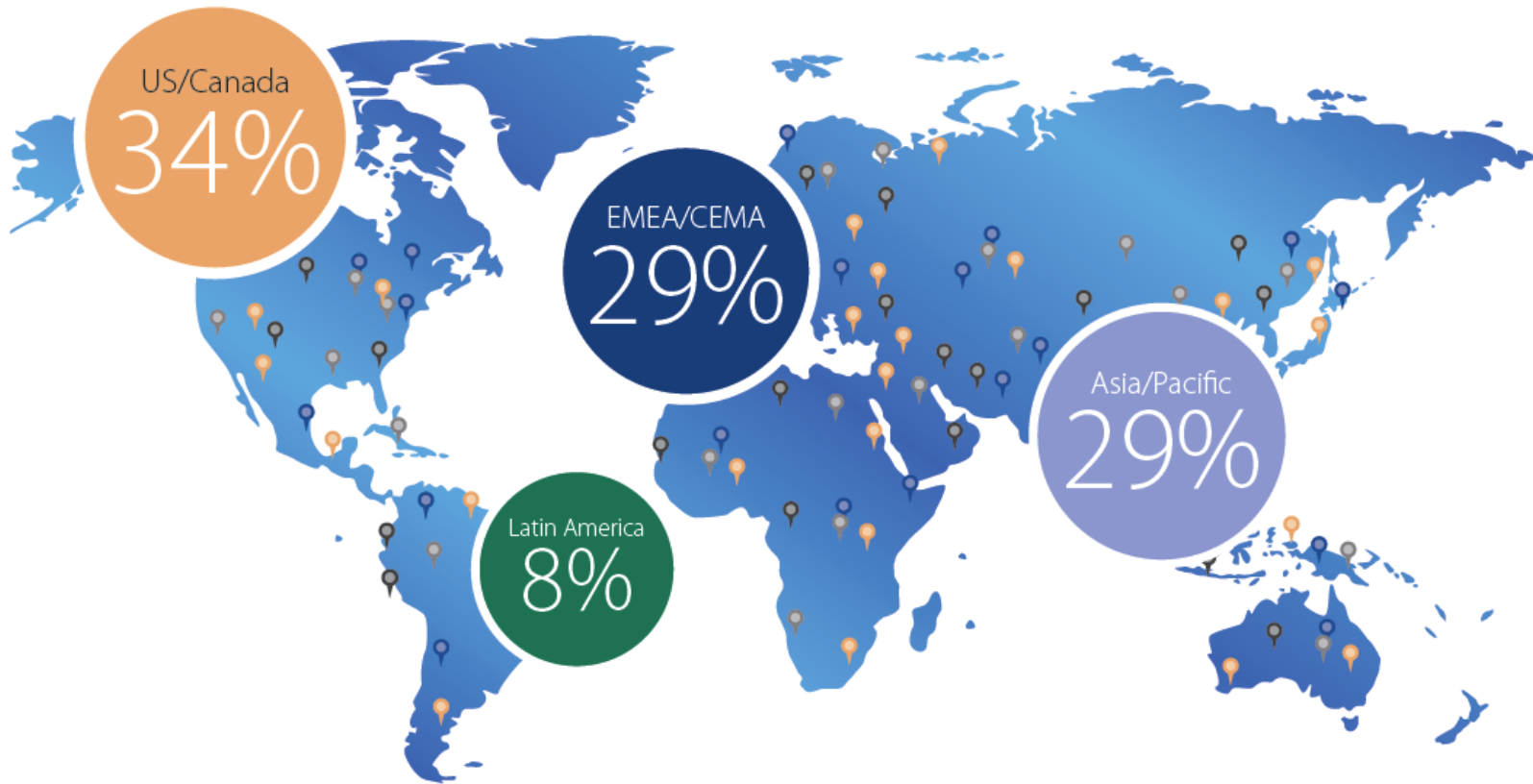
Pete Lindstrom

Vice President, Security Strategies
IT Executive Program, IDC



- Over 25 years in InfoSec, IT, Finance
- Tech Risk Pro performing reading, writing, 'rithmetic on risk and security matters
- Former Marine (Gulf War veteran), 'Big Six' IT Auditor (PwC), Internal Auditor (GMAC Mortgage), Security Architect & Director (Wyeth)
- BBA Finance, University of Notre Dame; reformed CISA and CISSP

1,100 Research Analysts Located All Over The World



Identifying How Firms Manage Cybersecurity Investment

Tyler Moore

Tandy School of Computer Science
University of Tulsa, USA
tyler-moore@utulsa.edu

Scott Dynes Frederick R. Chang

Darwin Deason Institute for Cyber Security
Southern Methodist University, USA
{scottd, chang}@smu.edu

Abstract

We report on a set of 40 semi-structured interviews with information security executives and managers at a variety of firms and government agencies. The purpose of the interviews was to learn more about how organizations make cybersecurity investment decisions: how much support they receive to execute their mission, how they prioritize which threats to defend against, and how they choose between competing security controls. We find that most private sector executives believe that their firms adequately fund cybersecurity, but that finding qualified personnel inhibits the pace of adoption of new controls. Most firms do not calculate return on investment (ROI) or other outcome-based quantitative investment metrics; instead, they opt for process-based frameworks such as NIST and COBIT to guide strategic investment decisions. Finally, we note that CISOs in government face considerable challenges compared to their private-sector counterparts.

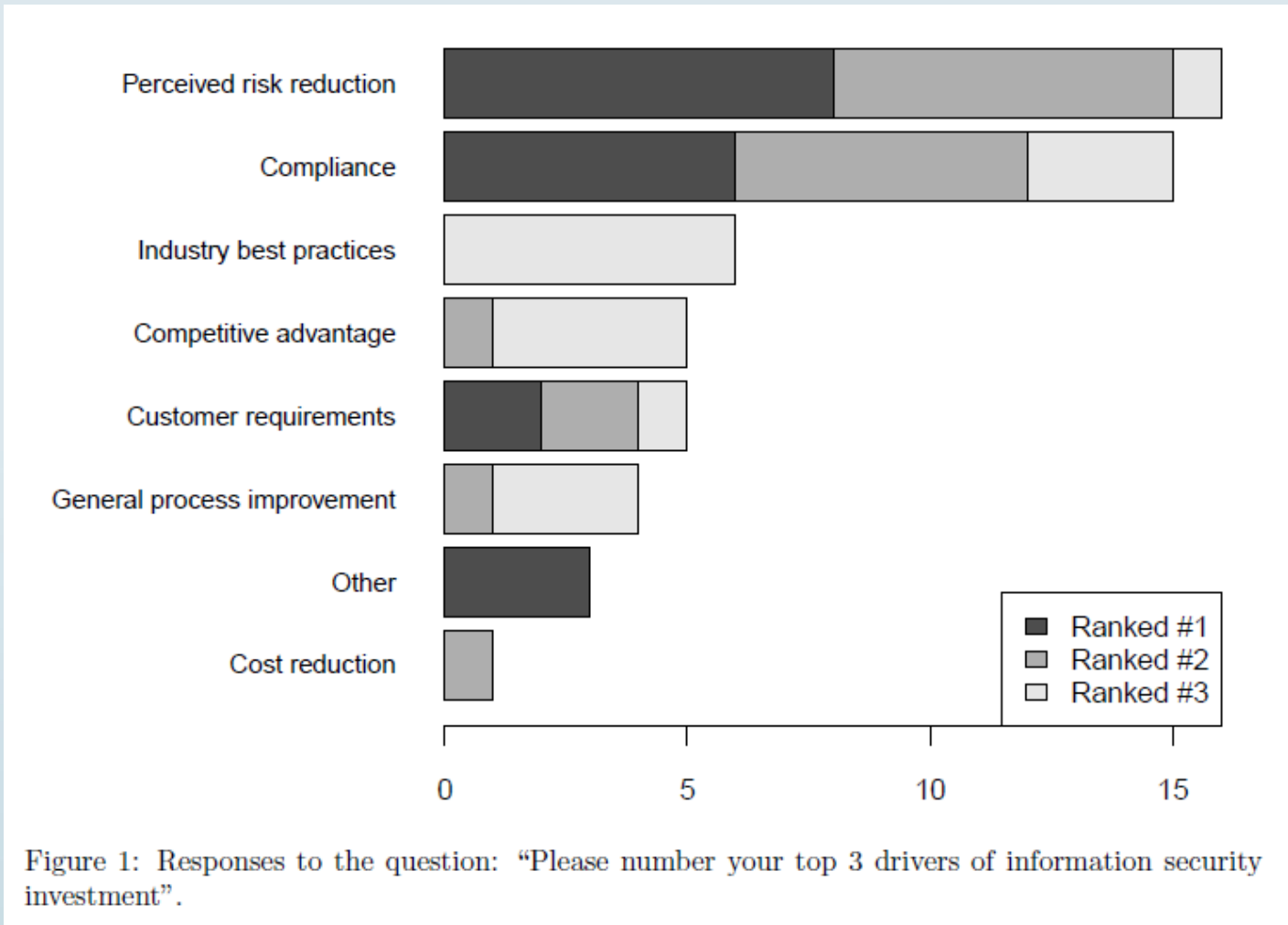


Figure 1: Responses to the question: “Please number your top 3 drivers of information security investment”.

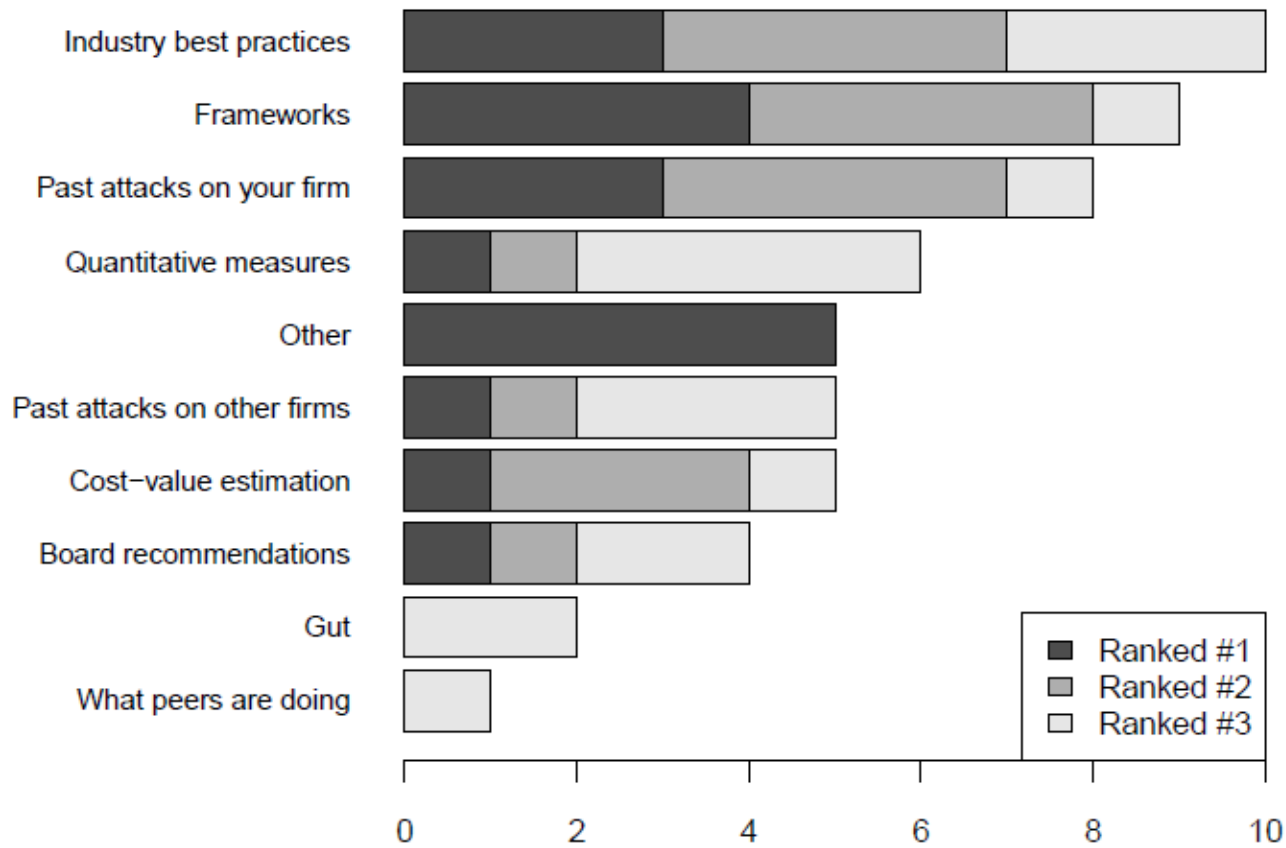


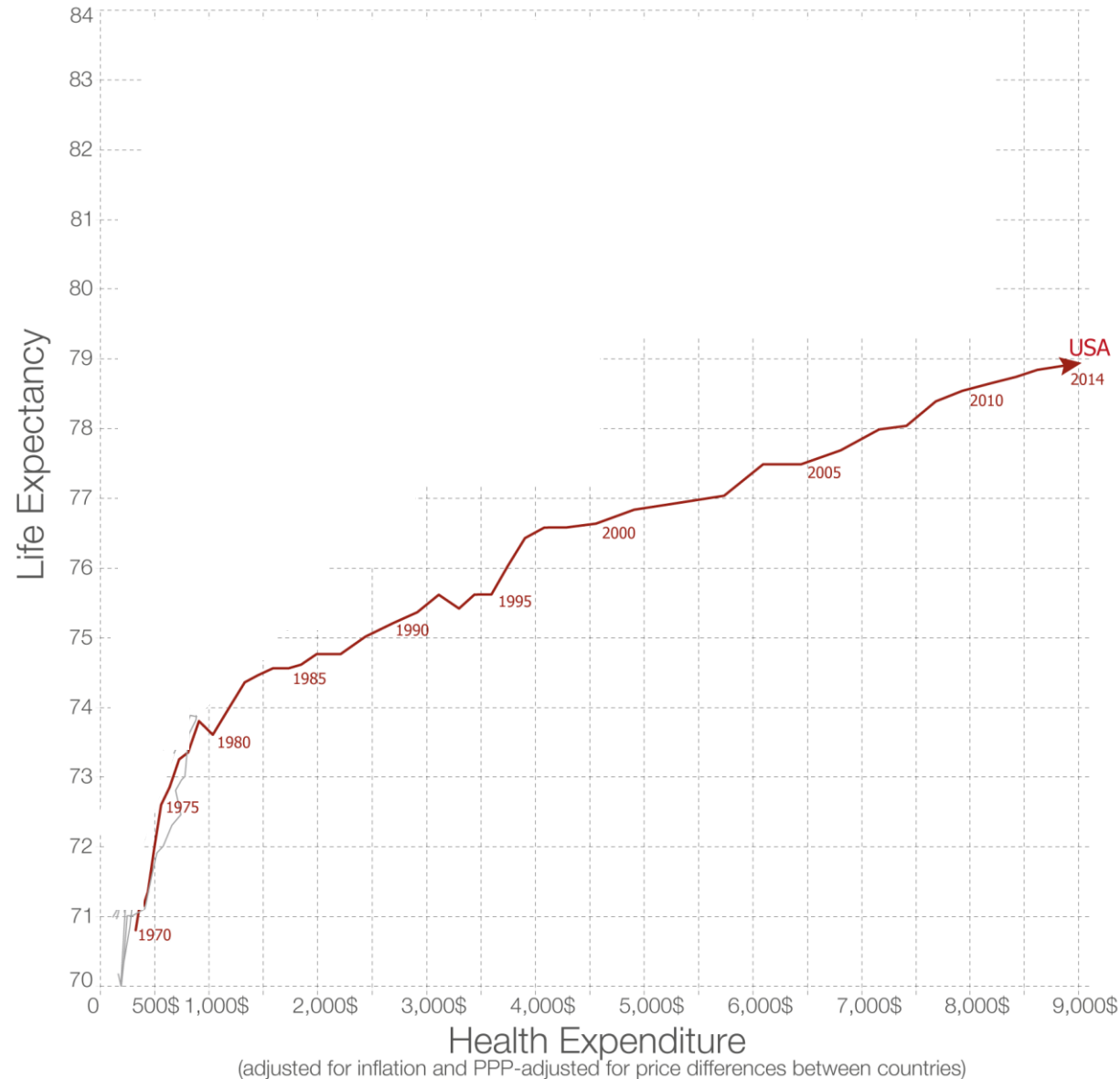
Figure 2: Responses to the question: “Please number your top 3 prioritization approaches”.

Fundamental Cybersecurity Challenge

*How can I tell how effective (or ineffective)
my security program is?*

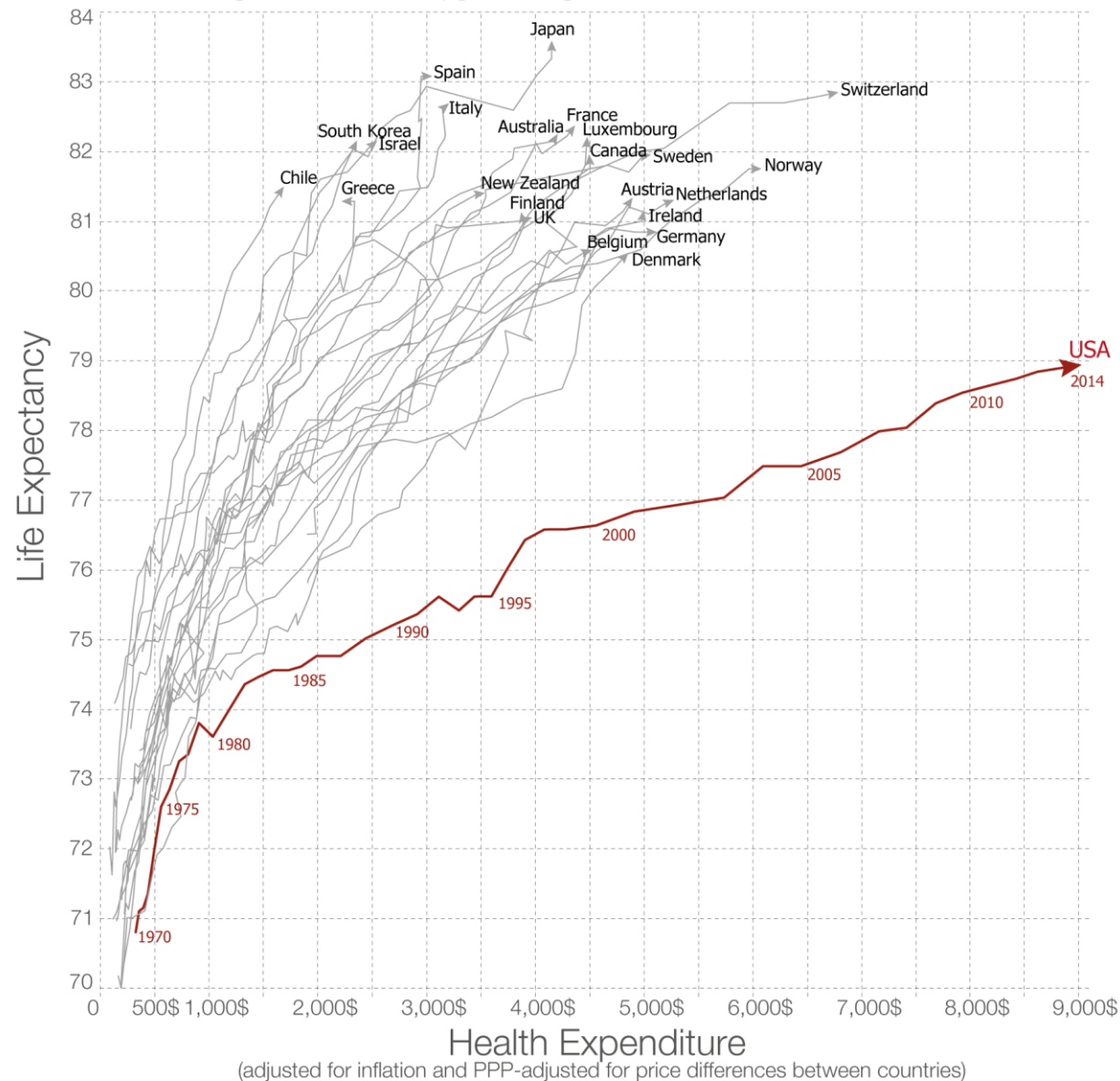
Life expectancy vs. health expenditure over time (1970-2014)

Health spending measures the consumption of health care goods and services, including personal health care (curative care, rehabilitative care, long-term care, ancillary services and medical goods) and collective services (prevention and public health services as well as health administration), but excluding spending on investments. Shown is total health expenditure (financed by public and private sources).

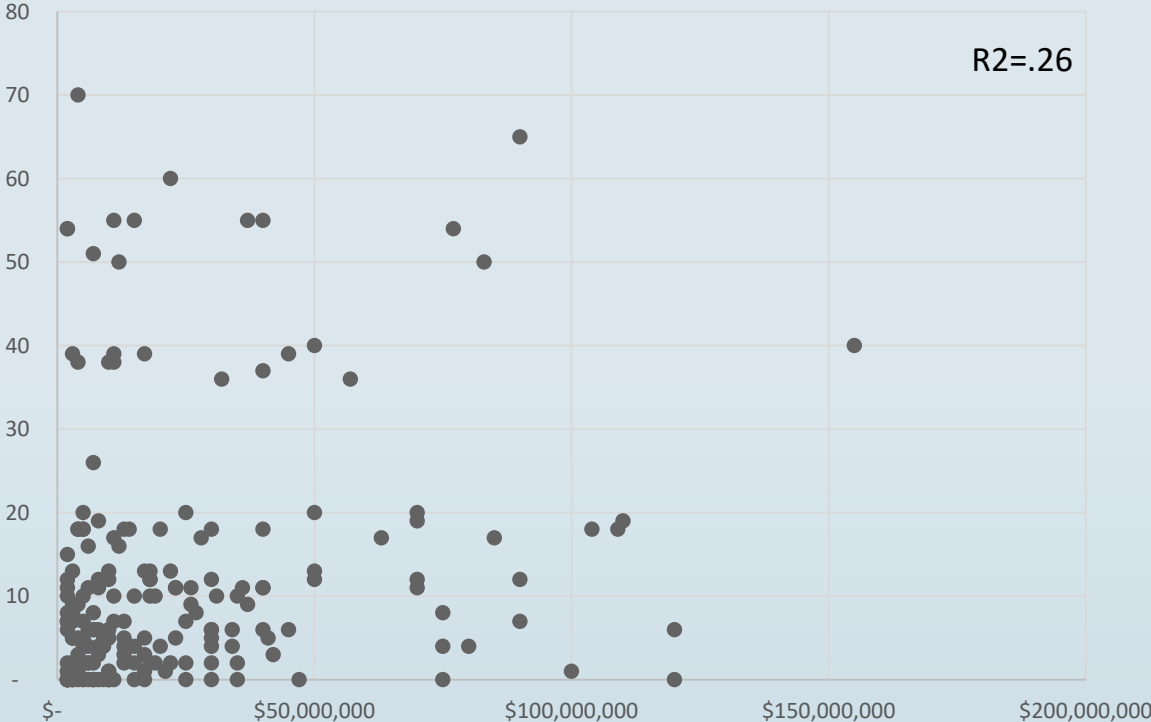


Life expectancy vs. health expenditure over time (1970-2014)

Health spending measures the consumption of health care goods and services, including personal health care (curative care, rehabilitative care, long-term care, ancillary services and medical goods) and collective services (prevention and public health services as well as health administration), but excluding spending on investments. Shown is total health expenditure (financed by public and private sources).

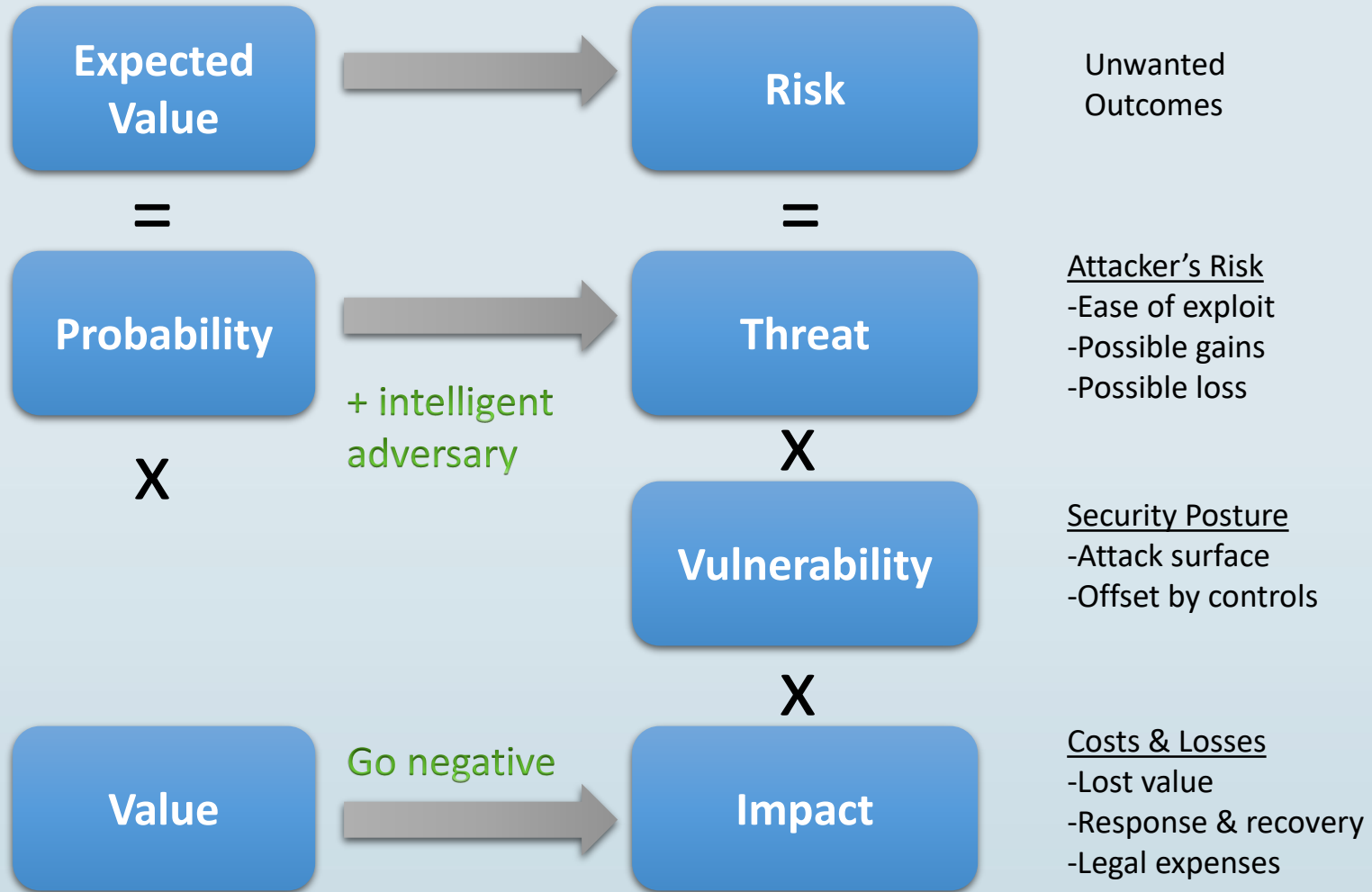


Higher Spending != Fewer Incidents



Key Risk Indicators are repeatable measures (observations) collected from pertinent IT environment(s) that provide insight into the likelihood and impact associated with unwanted outcomes.

The Risk Equation



How Risk Changes

Vulnerabilities

Vuln increases when...	Vuln decreases when...
Add users	Delete/disable users
Open ports	Close ports
Add systems	Remove systems
Add apps/services	Remove apps/services
Add administrators	Remove administrators

Threats

Threat increases when...	Threat decreases when...
Lower attack costs	Increase attack costs
Add system access	Remove system access
Disclosing vulnerabilities	Prosecuting hackers

Impact

Impact increases when...	Impact decreases when...
Increased regulations	Decreased regulations
Increased value of systems	Decreased value of systems

Calculating Impact / Losses

What's a Life Worth?

9/11 FAMILY PAYOUTS In a formula that accounted for lost income, families of victims who made more money received larger awards, on average.

BY INCOME LEVEL	AVERAGE AWARD	NUMBER OF CLAIMS
No income	\$ 788,022	17
\$24,999 or less	1,102,135	163
\$25,000 to 99,000	1,520,155	1,591
\$100,000 to 199,000	2,302,235	633
\$200,000 to 499,999	3,394,625	310
\$500,000 to 999,999	4,749,654	89
\$1 million to 1,999,999	5,671,816	52
\$2 million to 3,999,999	6,253,705	17
\$4 million and more	6,379,288	8

BY SEX	AVERAGE AWARD	NUMBER OF CLAIMS
Female	1,443,717	692
Male	2,283,916	2,188

BY OCCUPATION	AVERAGE AWARD	NUMBER OF CLAIMS
Food workers	1,351,968	97
Fire department	1,635,081	342
Technology/computers	1,814,290	130
Finance	2,456,521	1,669

Source: Sept. 11 Victim Compensation Fund of 2001

THE NEW YORK TIMES

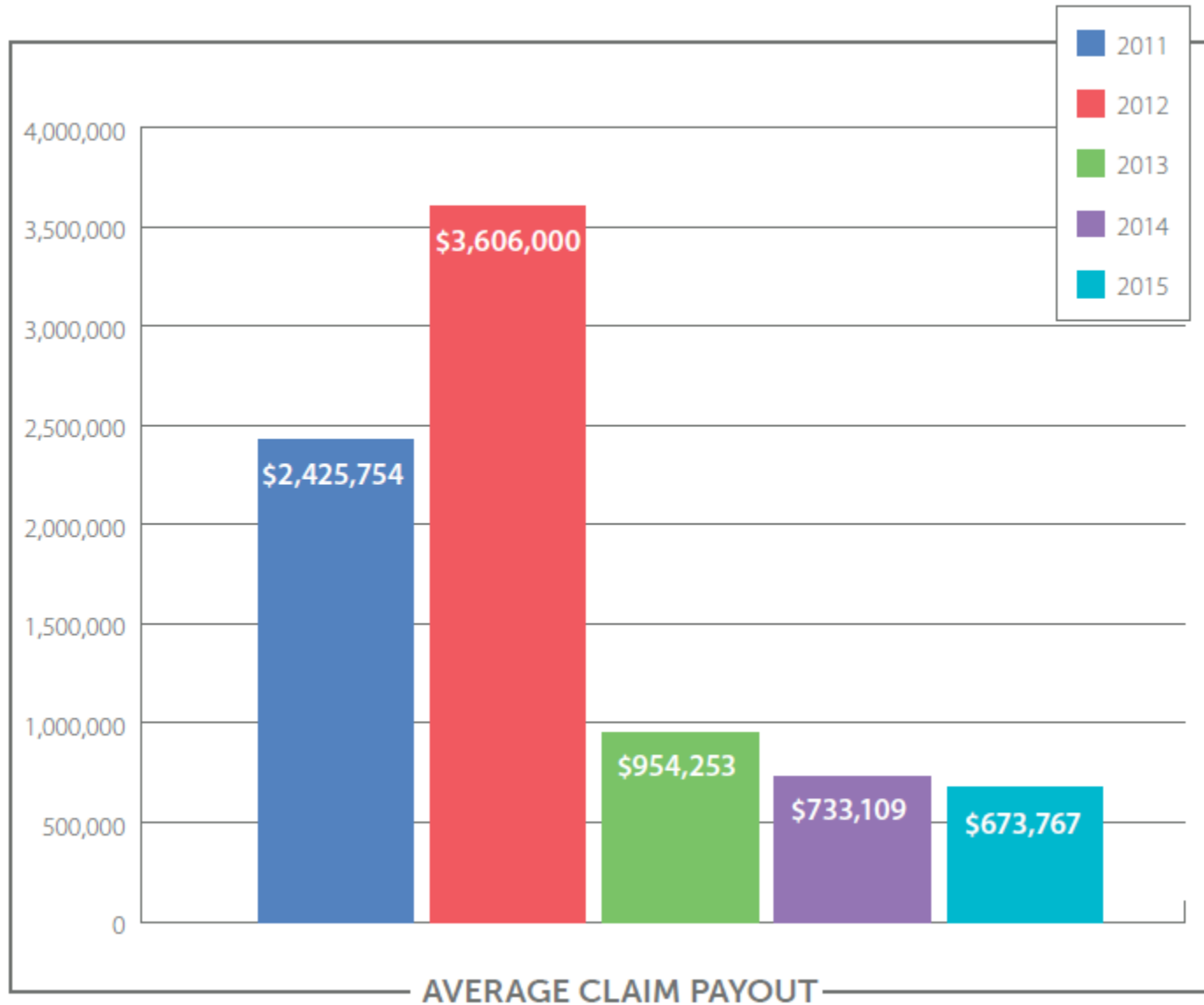


Table 2. Cost by event type (in millions)

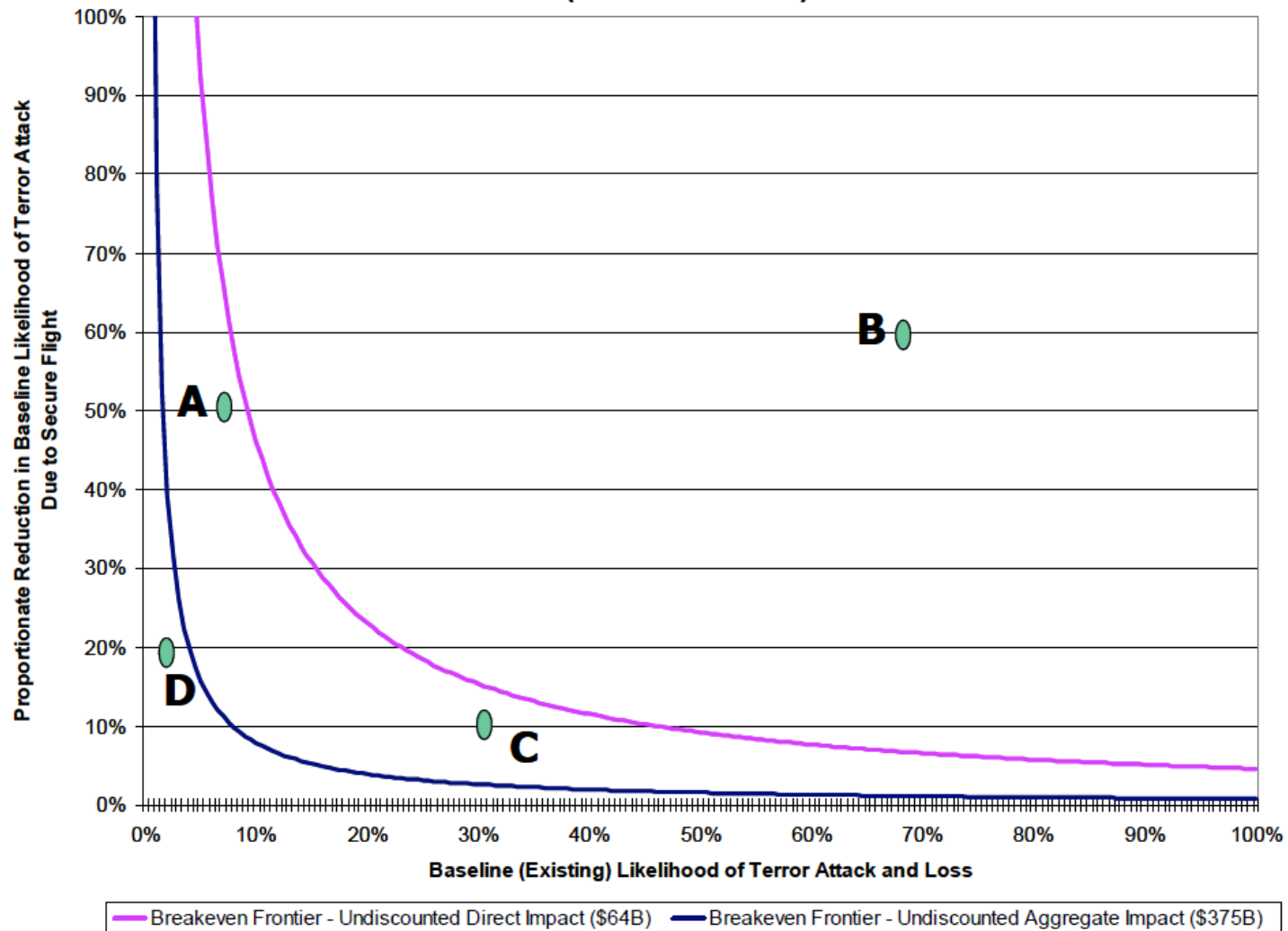
Event type	N	Mean	SD	Median	Min ^a	Max
Data Breach	602	5.87	35.70	0.17	0.00	572
Security Incident	36	9.17	27.02	0.33	0.00	100
Privacy Violation	234	10.14	55.41	1.34	0.00	750
Phishing	49	19.99	105.93	0.15	0.01	710
Total	921	7.84	47.28	0.25	0.00	750

^aValues are presented in millions of dollars and therefore, any zero values are artifacts of rounding functions.

Willingness to Pay

Equifax-style breach	1,840,938
Employees without computer access for 3 days	1,492,487
Breach is top news for mainstream media outlets	1,291,838
Public-facing corporate website unavailable for 3 days	1,036,116
Leak of a significant number of credit card records	799,867
Unrecoverable wire-transfer loss of \$2.5 million	511,113
IT systems are source/conduit of major attack against partner	478,357
Ecommerce website taken down by DDoS attack for 4 hours	475,814
Leak of key intellectual property (e.g. product docs, source code, etc)	417,814
Memory read by Meltdown/Spectre or similar exploit	62,018
Ransomware infection of 5 senior executives	57,203
Fraudulent order for \$100k worth of unrecoverable shipped goods	28,227

Secure Flight Breakeven Frontier for Risk Reduction of Aviation Terror Attack Likelihood, by Losses Due to Successful Attack (Undiscounted)



Calculating Likelihood / Frequency

You are doing it anyway...

Expression	25%	Median	75%	IQR	Expression	25%	Median	75%	IQR
Always	99.6	99.7	99.8	.3	Not often	10.3	19.7	24.8	14.5
Almost always	89.7	91.7	95.2	5.5	Not very often	5.3	10.1	19.6	14.3
Certain	98.7	99.6	99.8	1.1	Possible	7.5	38.5	50.2	42.7
Almost certain	87.5	90.2	95.0	7.5	Impossible	.2	.3	.5	.3
Very frequent	75.3	82.6	89.7	14.5	High chance	77.5	80.4	80.1	11.7

Expression	25%	Median	75%	IQR
Very high probability	89.8	92.5	95.2	5.4
High probability	77.1	82.3	87.2	10.1
Moderate probability	40.1	52.4	58.7	18.5
Low probability	7.8	15.0	22.3	14.5
Very low probability	1.9	4.9	7.6	5.7
Improbable	7.6	12.5	22.3	14.7
Very improbable	1.5	4.8	7.5	5.9
Very often	77.5	82.8	89.9	12.4
Often	65.0	72.5	75.4	10.4
More often than not	57.1	59.8	60.4	3.3
As often as not	49.8	50.0	50.3	.6
Less often than not	34.8	40.0	42.7	7.9
Seldom	7.4	10.2	17.5	10.1
Very seldom	3.2	4.9	7.7	4.5
Rarely	3.6	7.2	10.0	6.5
Very rarely	1.2	3.0	5.0	3.8
Almost never	1.2	2.9	4.6	3.4
Never	.1	.3	.4	.3

Source: Quantifying Probabilistic Expressions, Mosteller & Youtz

2013

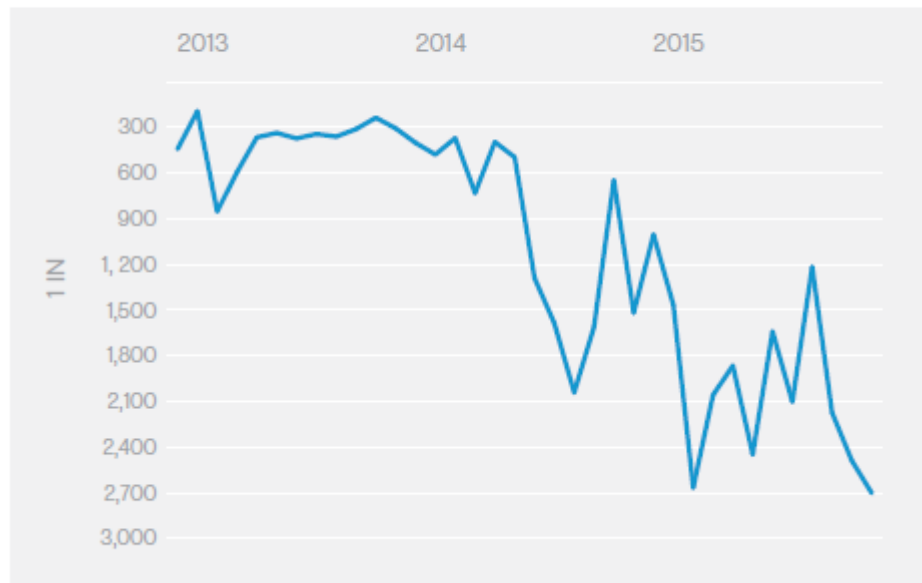
2014

2015

Phishing Rate

► Phishing numbers in 2015 continued to fluctuate, but remained in gradual decline throughout the year.

3.7
Million

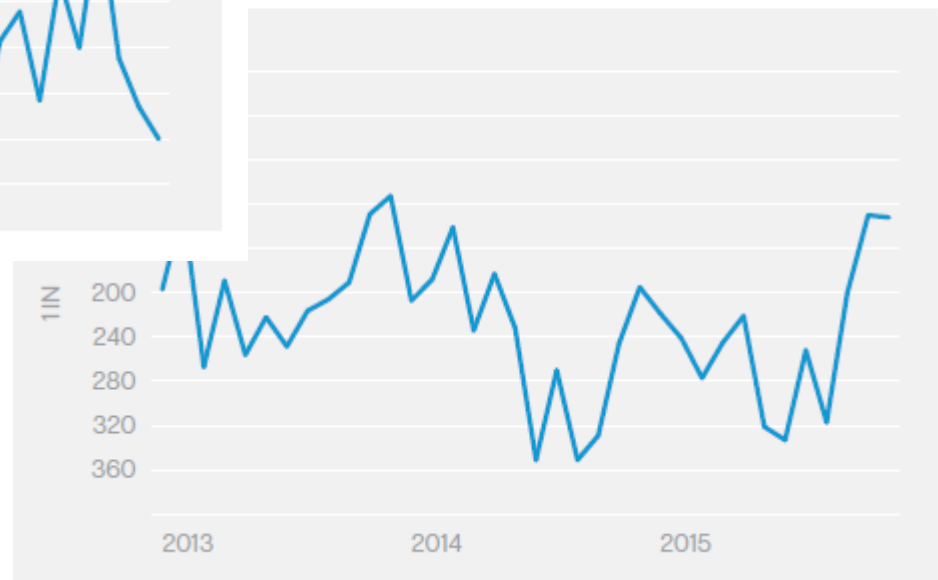


Further Classified as
Malware

1.2
Million

Email Traffic in Which Virus Was

Malware rate for 2015 increased since 2014. Email is a primary medium for cybercriminals.



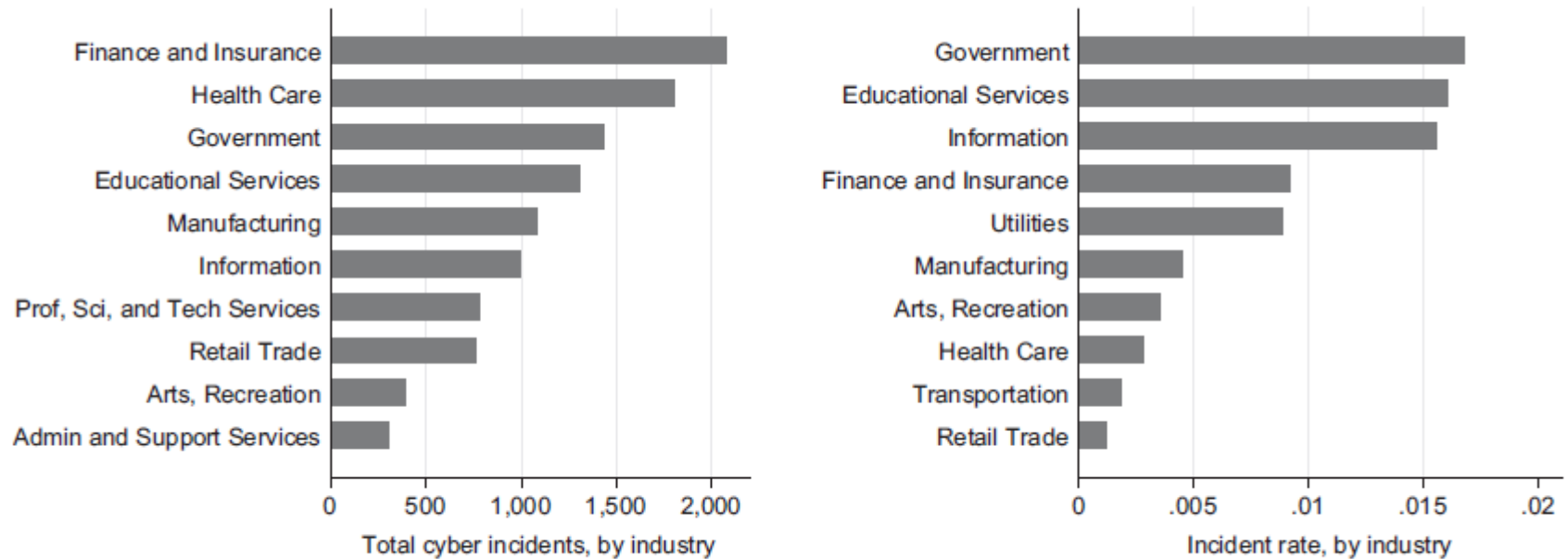


Figure 3. Cyber incidents, and rates, by industry.

While in essence, this article represents a descriptive analysis of a single dataset (rather than causal inference), we believe that it does provide relevant and important findings. For example, **by comparing observed cyber events with the total number of firms within an industry, this research provides one of the first true estimates of risk**, by industry type. Further, our use of cost data enables us to provide a unique and novel analysis of the scope and magnitude of cyber events, as a function of firm revenues, and other forms of loss, theft, and waste.

Key Risk Indicators are repeatable measures (observations) collected from pertinent IT environment(s) that provide insight into the likelihood and impact associated with unwanted outcomes.

An Analogy: Auto Accidents

Table 2
People Killed and Injured, and Fatality and Injury Rates, 2006–2015

Year	Killed	Resident Population (Thousands)	Fatality Rate per 100,000 Population	Licensed Drivers (Thousands)	Fatality Rate per 100,000 Licensed Drivers	Registered Motor Vehicles (Thousands)	Fatality Rate per 100,000 Registered Vehicles	Vehicle Miles Traveled (Billions)	Fatality Rate per 100 Million VMT
					Killed				
2006	42,708	298,380	14.31	202,810	21.06	251,415	16.99	3,014	1.42
2007	41,259	301,231	13.70	205,742	20.05	257,472	16.02	3,031	1.36
2008	37,423	304,094	12.31	208,321	17.96	259,360	14.43	2,977	1.26
2009	33,883	306,772	11.05	209,618	16.16	258,958	13.08	2,957	1.15
2010	32,999	309,347	10.67	210,115	15.71	257,312	12.82	2,967	1.11
2011	32,479	311,719	10.42	211,875	15.33	265,043	12.25	2,950	1.10
2012	33,782	314,103	10.76	211,815	15.95	265,647	12.72	2,969	1.14
2013	32,893	316,427	10.40	212,160	15.50	269,294	12.21	2,988	1.10
2014	32,744	318,907	10.27	214,092	15.29	274,805	11.92	3,026	1.08
2015	35,092	321,419	10.92	218,084	16.09	281,312	12.47	3,095	1.13

What are the denominators?

➤ Company

- Of a certain size (revenue, employees, market cap, etc)
- In a certain industry

➤ Assets

- Lines of business
- Networks (dc, branch, soho, store, etc)
- Applications, Servers, Endpoints, Users

➤ Activity

- Flows, connections, sessions
- Messages, transactions

Collect Asset and State Information to Normalize IT Environment Data

- Number of **servers**, physical and/or logical.
- Number of **open ports** that are listening for connections on the servers.
- Number of **client endpoints**, such as desktops, laptops, tablets, and mobile devices used to communicate with applications available to organization's users.
- Number of **applications** in use by the organization.
- Number of **unique users** that have one or more accounts in the environment.
- Number of **unique user accounts** that exist for all applications and systems in the environment.
- Number of **executable files** to identify the software objects that may be targeted for attack.
- Number of **known vulnerabilities** throughout the entire environment.

Start with Existing Inline Security Solution Data



- **Endpoint antimalware solutions** scan inbound executable files for signs that they are malware.
- **Firewalls** make deterministic decisions about network connection requests. Many also apply more logic associated with higher layers.
- **Intrusion prevention solutions** evaluate network traffic looking for indicators of attacks.
- **Email security gateways** evaluate email messages for signs that they are spam or contain malware or links to malware.
- **Secure web gateways** evaluate web URLs and web pages for malicious content.

Collect Event Set Information



- Number of **network flows** to track the volume of activity at the network level.
- Number of **sessions** to identify the number of users and/or sources of connections to applications that occur within a specific time period.
- Number of **messages** associated with email and other communication applications.
- Number of **files transmitted/received** that are used for typical productivity purposes.
- Number of **active users/accounts** to identify the population from which threats occur.
- Number of **active IP addresses** (src/dest) to identify active resources that may be acting as threat sources or vulnerable targets, or both.

- Reviewing quarantined files or data for indicators that they are benign.
- Evaluating the outcomes for sequential controls and determining whether true positives at the downstream control were missed by the upstream control.
- Sampling some set of events or objects associated with a control and scrutinizing the objects or data for signs of malice.
- Reviewing help desk calls that are resolved by disabling various security features, creating new firewall rules, or some other key procedures.
- Threat Hunting: Sampling and evaluating IT assets for signs of infection or compromise.

Putting the Numbers Together

IT Security Control Efficacy



	Total population
True condition	condition positive
	condition negative

https://en.wikipedia.org/wiki/Matthews_correlation_coefficient

IT Security Control Efficacy



		Predicted condition	
		Predicted Condition positive	Predicted Condition negative
True condition	condition positive	True positive	False Negative (Type II error)
	condition negative	False Positive (Type I error)	True negative

https://en.wikipedia.org/wiki/Matthews_correlation_coefficient

IT Security Control Efficacy

		Predicted condition			
		Predicted Condition positive	Predicted Condition negative	Prevalence $= \frac{\Sigma \text{Condition positive}}{\Sigma \text{Total population}}$	
True condition	condition positive	True positive	False Negative (Type II error)	True positive rate (TPR), Sensitivity, Recall $= \frac{\Sigma \text{True positive}}{\Sigma \text{Condition positive}}$	False negative rate (FNR), Miss rate $= \frac{\Sigma \text{False negative}}{\Sigma \text{Condition positive}}$
	condition negative	False Positive (Type I error)	True negative	False positive rate (FPR), Fall-out $= \frac{\Sigma \text{False positive}}{\Sigma \text{Condition negative}}$	True negative rate (TNR), Specificity (SPC) $= \frac{\Sigma \text{True negative}}{\Sigma \text{Condition negative}}$
Accuracy (ACC) = $\frac{\Sigma \text{True positive} + \Sigma \text{True negative}}{\Sigma \text{Total population}}$		Positive predictive value (PPV), Precision $= \frac{\Sigma \text{True positive}}{\Sigma \text{Test outcome positive}}$	False omission rate (FOR) = $\frac{\Sigma \text{False negative}}{\Sigma \text{Test outcome negative}}$	Positive likelihood ratio (LR+) = $\frac{\text{TPR}}{\text{FPR}}$	Diagnostic odds ratio (DOR) = $\frac{\text{LR+}}{\text{LR-}}$
		False discovery rate (FDR) $= \frac{\Sigma \text{False positive}}{\Sigma \text{Test outcome positive}}$	Negative predictive value (NPV) $= \frac{\Sigma \text{True negative}}{\Sigma \text{Test outcome negative}}$	Negative likelihood ratio (LR-) = $\frac{\text{FNR}}{\text{TNR}}$	

https://en.wikipedia.org/wiki/Matthews_correlation_coefficient

Key Risk Indicators (KRIs)

Control Outcome	Population	Efficacy / Errors	Normalized
Endpoint Antimalware allowed/denied	File Objects	Malware blocked (TP); Legitimate file allowed (TN); Legitimate file blocked (FP); Malware allowed (FN)	Number of files transmitted Total files Number of endpoints Number of users Business Unit/Department
Firewall connections allowed/denied	Network Flows/Connections	Connection blocked (TP); Legitimate connection allowed (TN); Legitimate connection blocked (FP); Connection allowed (FN)	Number of flows Number of active IP address Number of open ports Number of applications Business unit/Department
Intrusion Prevention flows allowed/denied	Network Flows/Connections File Objects	Connection/malware blocked (TP); Legitimate connection/file allowed (TN); Legitimate connection/file blocked (FP); Connection/malware allowed (FN)	Number of flows Number of active IP address Number of open ports Number of files transmitted Number of applications Business unit/Department
Email Security messages allowed/denied	Email Messages	Phish/malware blocked (TP); Legitimate email allowed (TN); Legitimate email blocked (FP); Phish/malware allowed (FN)	Number of messages Number of users
Secure Web Gateway sessions allowed/denied	Web Sessions (outbound)	Malicious/inappropriate Web blocked (TP); Legit Web session allowed (TN); Legit Web session blocked (FP); Malicious/inappropriate Web allowed (FN)	Number of Web sessions Number of users

Opportunity knocks...

- Control efficacy that leverages well-established concepts like confusion matrices and sensitivity and specificity measures to compare controls.
- Infection/compromise rate to identify the number of infections per individual assets, such as endpoints.
- Controls per transaction that identifies the number of inline security tests performed on average for every event on the network.
- Incidents per billion events to identify the number of unwanted outcomes that occur for every billion events evaluated.
- Relative risk ratio of one environment to another, again leveraging established concepts in epidemiology.

Digital Security Strategic Metrics



- 1. Transaction Value (TV)** - (Total Value of IT and Information Assets \$ / Total Transactions)
- 2. Transaction Cost (TC)** - (Total Cost of IT and Information Assets \$ / Total Transactions)
- 3. Controls per Transaction (CPT)** - (Total Number of Inline Control Events / Total Transactions)
- 4. Cost per Control (CPC)** - (Total Cost of Control \$ / Total Number of Inline Control Events)
- 5. Security to Value Ratio (STV)** - (Total Security Costs \$ / Total Value of IT and Information Assets \$)
- 6. Loss to Value Ratio (LTV)** - (Total Losses \$ / Total Value of IT and Information Assets \$)
- 7. Control Effectiveness Ratio (CE)** - ((Good Allowed Control Events + Bad Denied Control Events) / Total Number of Inline Control Events)
- 8. Incidents per Million (IPM); Incidents per Billion (IPB)** - ((Total Number of Incidents / Total Transactions) x One Million or Billion)
- 9. Incident Prevention Rate (IPR)** - $(1 - (\text{Total Incidents} / (\text{Good Denied} + \text{Total Incidents})))$
- 10. Risk Aversion Ratio (RAR)** - (Good Denied / Total Incidents)

Five-Hundred Life-Saving Interventions and Their Cost-Effectiveness

Risk Analysis, Vol. 15, No. 3, 1995

Cost-Effectiveness of Saving Lives

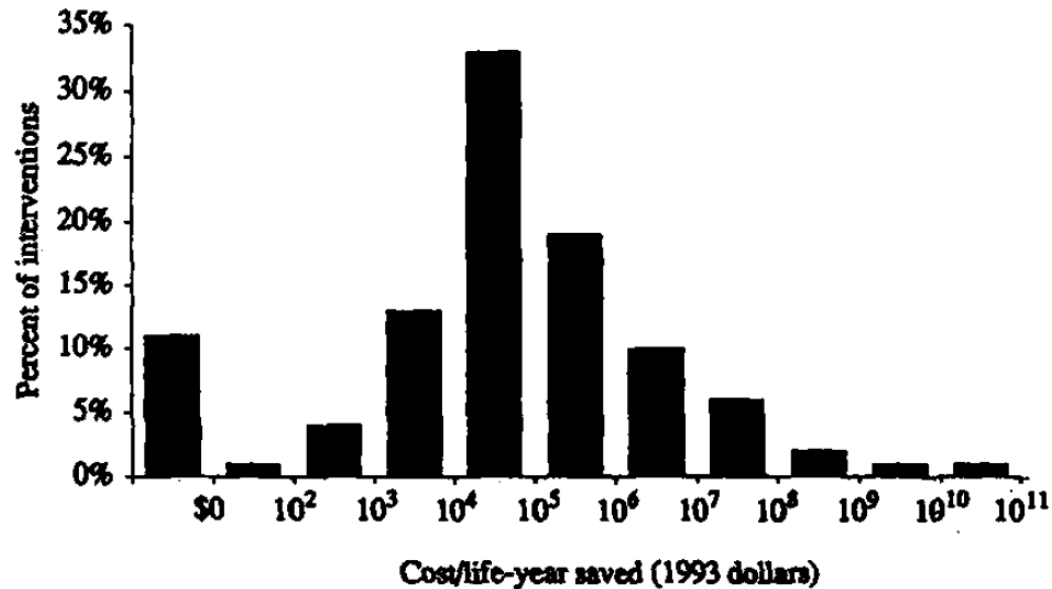


Fig. 1. Distribution of cost/life-year saved estimates ($n = 587$).

Tammy O. Tengs,¹ Miriam E. Adams,² Joseph S. Pliskin,^{3,6} Dana Gelb Safran,⁴
Joanna E. Siegel,^{5,7} Milton C. Weinstein,^{6,7} and John D. Graham^{6,7}

*The One Security Metric to rule
them all...*



Risk Reduced per Unit Cost

RRUC= Risk Reduced (\$) / Total Cost of Ownership (\$)

where RR = Risk' - Risk *or* (probability*impact)' -
(probability*impact)

and TCO = Annualized Capital Costs (hardware,
software) + Labor + Maintenance + Service

Recap

- Start with existing inline security solution outcomes – antimalware infections, firewall drops, etc.
- Collect event set information for populations – flows, sessions, messages, files, etc.
- Incorporate false positive and false negative information with true positives and true negatives
- Collect asset and state information to normalize data – servers, applications, users, etc.
- Create ratios for more beneficial strategic uses of KRIs

Conclusion

- KRIs provide important objective measures of the strength of a security program.
- Organizations may be defining KRIs incorrectly for IT adversarial risk management in digital security.
- Further development of collected data will create opportunities to compare and contrast risk profiles across dissimilar environments and in benchmarking scenarios.
- Incorrect assumptions have stymied the use and validation of KRIs in digital security to date.



Pete Lindstrom
Vice President, Security Strategies
IT Executive Program, IDC
plindstrom@idc.com

Thanks!



ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?



ISSA

Information Systems Security Association
International

www.issa.org

Cyber Residual Risk Scoring

Michael F. Angelo – CRISC, CISSP

Chief Security Architect

Micro Focus | NetIQ Corporation

angelom@netiq.com

Agenda

- Where are we
- Modern Warfare
- Risk & Residual Risk Scoring
- What's Next?



Post Apocalypse

Cyber Survival



Cyber Survival




On the Verge of War

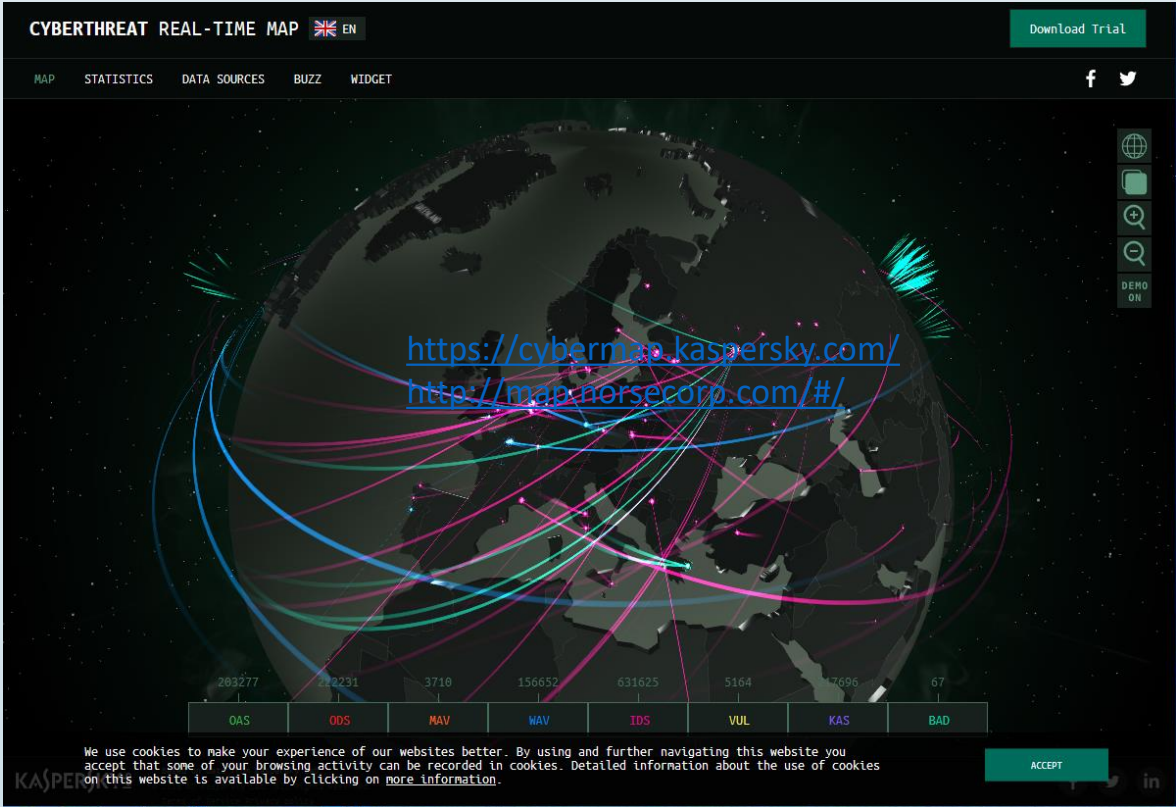
The Past 3 Years?

- # of cyber attacks
 - are you aware of?
 - How many were successful?
- What was the impact?
 - How much did it cost? (inc Fines)
 - How much PII was lost?

At War...

CYBERTHREAT REAL-TIME MAP  EN Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET f 🐦



<https://cybermap.kaspersky.com/>
<http://map.norsecorp.com/#/>

203277	22231	3710	156652	631825	5164	17696	67
OAS	ODS	MAV	WAV	IDS	VUL	KAS	BAD

We use cookies to make your experience of our websites better. By using and further navigating this website you accept that some of your browsing activity can be recorded in cookies. Detailed information about the use of cookies on this website is available by clicking on [more information](#). ACCEPT

KASPERSKY in

We Are At War

➤ Sun Tzu

- If you know the enemy and know yourself, you need not fear the result of a hundred battles.
- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
- If you know neither the enemy nor yourself, you will succumb in every battle.

Where do we fit?

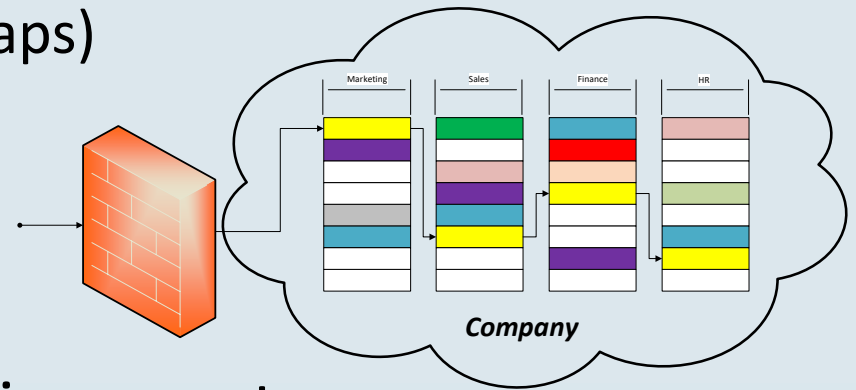
Do We Know The Enemy?

- Nation States
- Criminals
- Insiders
- Your Family

We Don't Know Who

Self Knowledge

- Cyber Defense
 - Inconsistent implementation
 - Verticals don't integrate (gaps)
- Changes to infrastructure
 - New technologies
 - New uses
- Unanticipated & re-occurring events



Sounds Familiar?

Do We Know Ourselves?

- Proof we know ourselves?
 - ❑ 146 days to detect
 - ❑ 2 to 1 people outside telling you have a problem
- How much do we spend every year, in security?

We Have a Problem....

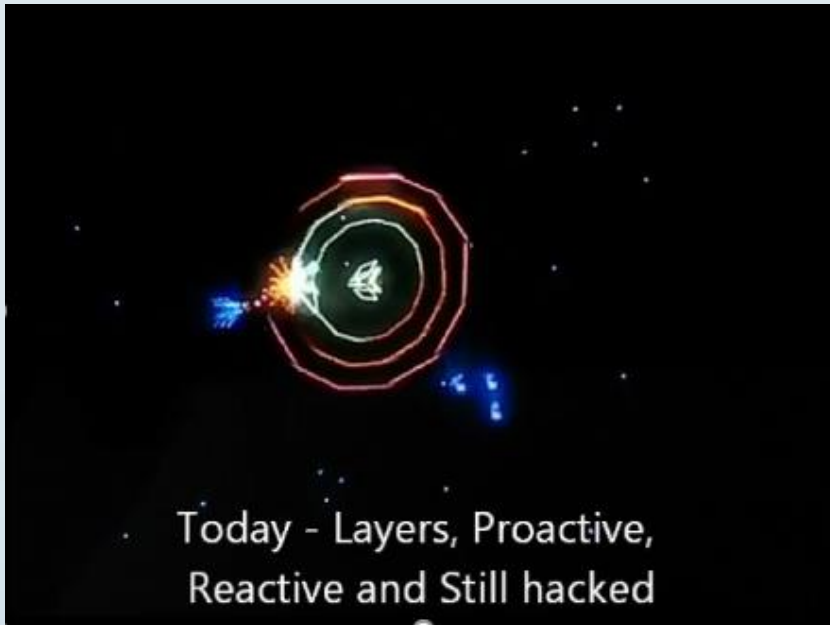
Are We Doomed?

Cyber Scoring Methodology

Past: Cyber Defense - Castle



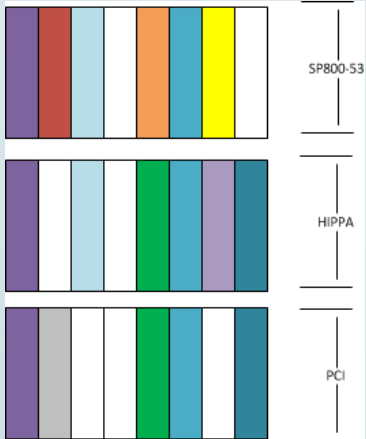
Today



Future: Rediscovering - Certs & Standards



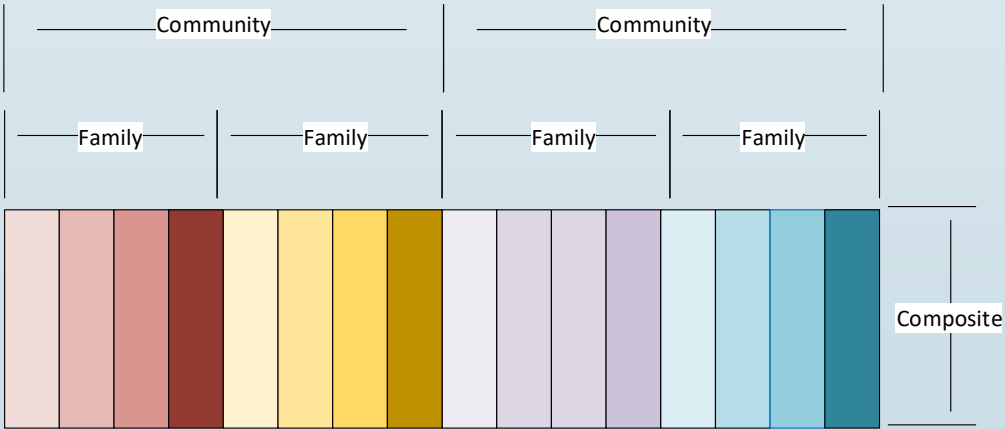
- How many security standards and certifications do we have?
- How many certified companies are you aware of that have been hacked?



Rediscovering Ourselves - Certs & Std



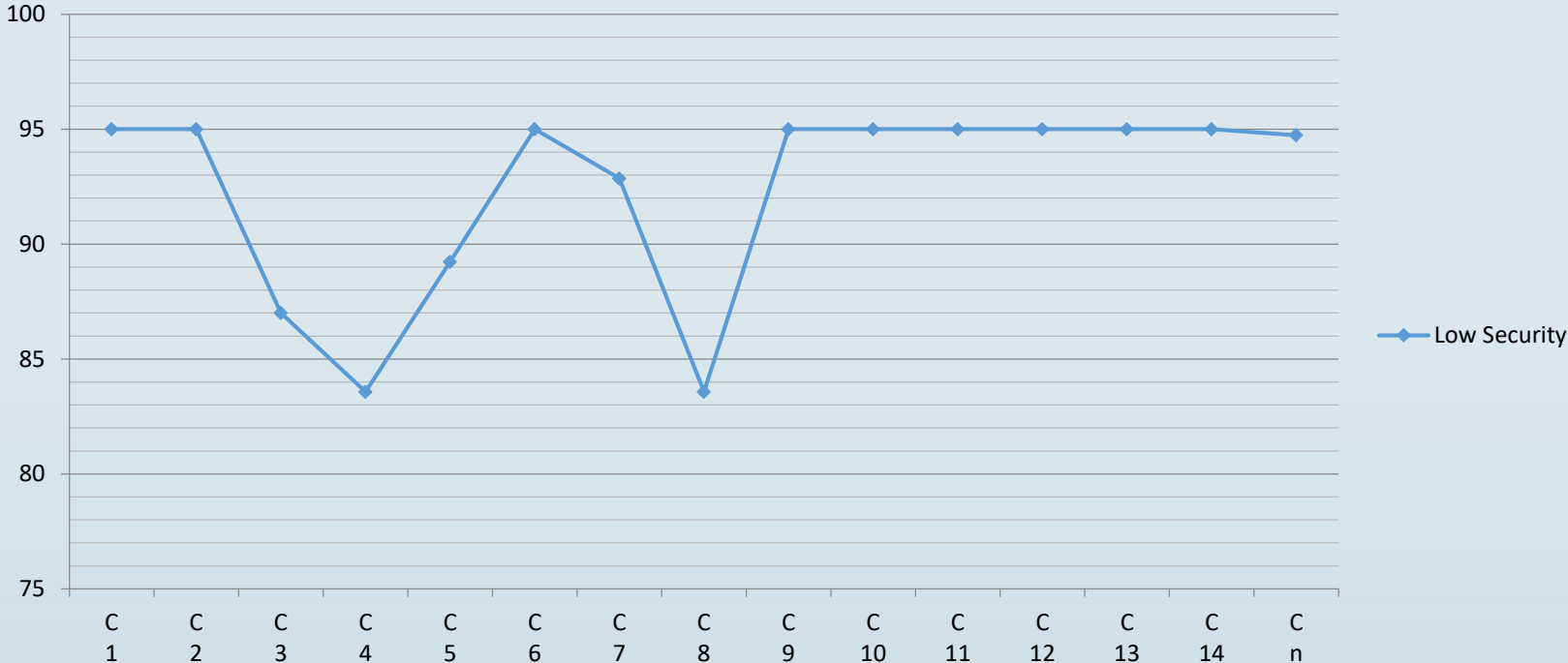
- What if we combined them?
 - ❑ Group complimentary
- Creating a Cyber Score
- Perform evidentiary audit



Rediscovering Ourselves - Certs & Std

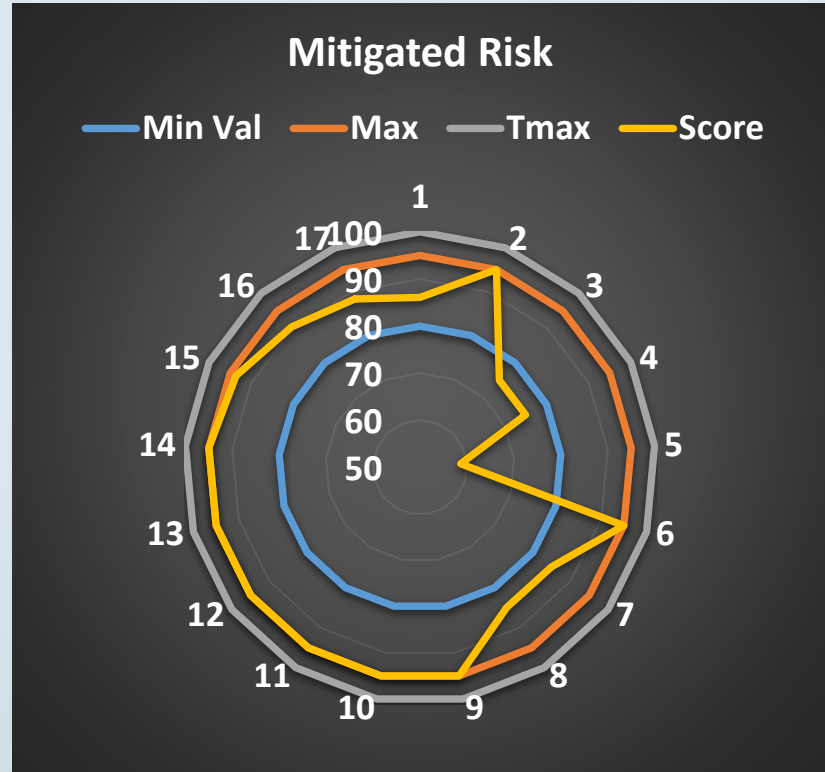


Cyber Risk Posture



Risk Score

Community	Min Val	Max	Tmax	Score
1	80	95	100	86
2	80	95	100	95
3	80	95	100	75
4	80	95	100	75
5	80	95	100	59
6	80	95	100	95
7	80	95	100	85
8	80	95	100	85
9	80	95	100	95
10	80	95	100	95
11	80	95	100	95
12	80	95	100	95
13	80	95	100	95
14	80	95	100	95
15	80	95	100	94
16	80	95	100	90
17	80	95	100	88

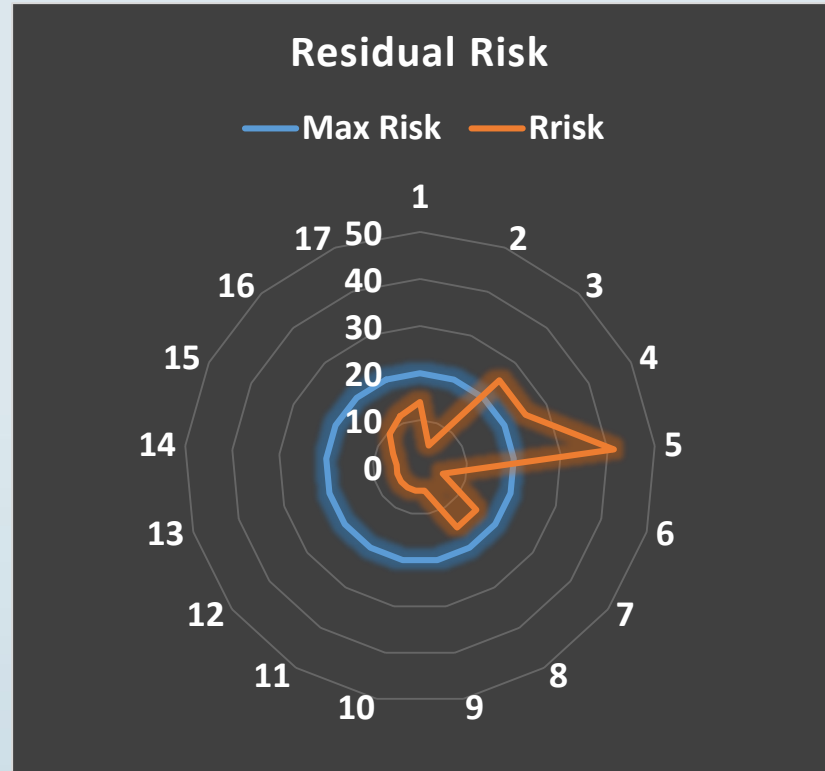


So ... Residual Risk



Residual Risk

Community	Max Risk	Risk
1	20	14
2	20	5
3	20	25
4	20	25
5	20	41
6	20	5
7	20	15
8	20	15
9	20	5
10	20	5
11	20	5
12	20	5
13	20	5
14	20	5
15	20	6
16	20	10
17	20	12



Corporate Diversity - Similar, But Unique...



- Must be Entity Centric Model and Results
 - ❑ Each Model may be as unique as each company
 - ❑ Not all company exposures are the same
- Not a bad thing, different infrastructures reduce attack surface

Attacks Are Inevitable

Benefits

- Understand Actual Cyber Risk Posture
 - ❑ Know Your Mitigation Landscape
 - ❑ Enables Mitigation Strategy
- Understand Compliance Posture
 - ❑ Map to Different Certifications
- You Have the Ability / Intelligence to Manage Your Environment

Survivability, But...

Rediscovering Ourselves

- Where to Improve (traditional):
 - Cost of Mitigation < benefit of mitigation
 - Likelihood of mitigation < likelihood of exploit
 - Risk that is left after all other risks are mitigated

Doesn't Help Us Know Our Enemy

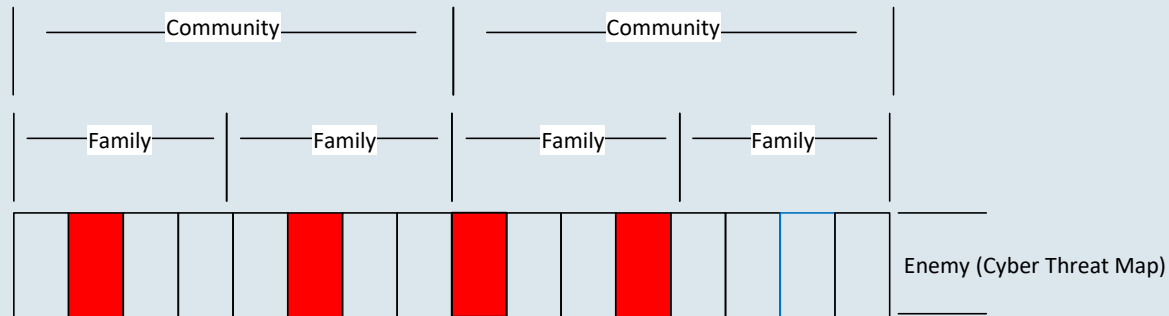
Getting To Know The Enemy?



If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

- Know them by their Works
- What if we could analyze all attacks
 - Identify infrastructure weaknesses exploited
 - Layer onto *Risk Posture*, with a Duplicate Template

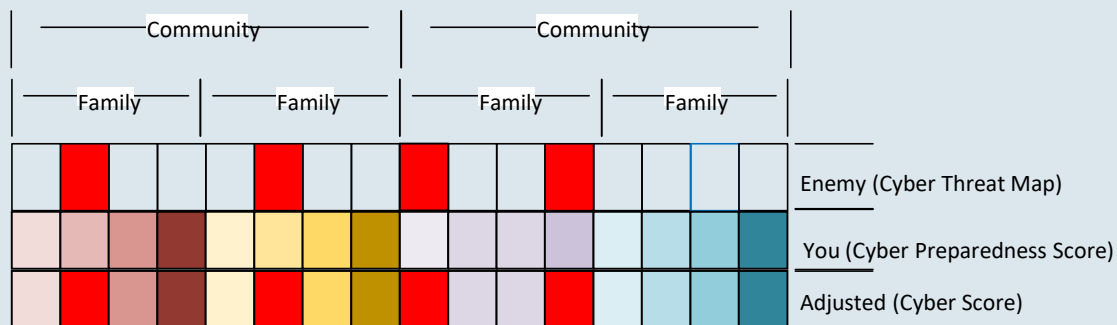
Knowing The Enemy: Cyber Attack Map



➤ Don't Know Who, But Know What...

- Successful attacks are analyzed
- Mapped based on impact to Cyber Preparedness elements

Putting It Together



- Attacks **MUST** be analyzed and mapped
 - ❑ Analysis based on attack elements
 - ❑ Result requires re-exam of components

What's Next?

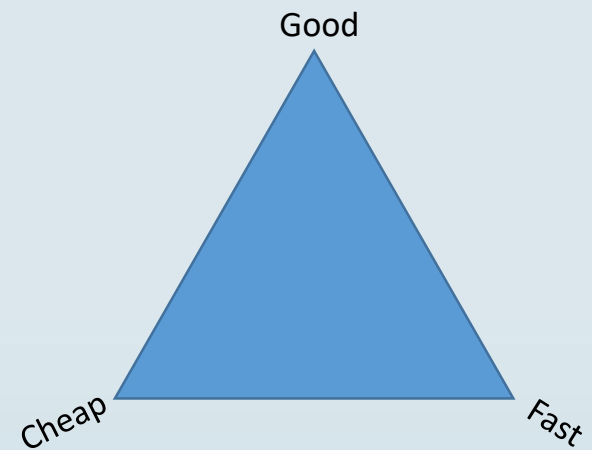
- We Know Ourselves,
- and We Know Our Enemy....

Are We Done?

Downside

➤ Requirements to Succeed

- Initial Analysis & Collection of Evidentiary Materials
- Change Control and Monitoring
- Ongoing Threat Landscape Analysis



Garbage In / Garbage Out

Where Are We?

- Need to change the way we operate to win.
 - ❑ Know Ourselves and Our Enemy via Cyber Scoring Methodology
- Results aren't static
 - ❑ we change, so will our enemy.
- We can control the battlefield

Imagine the future...

Imagine the Future...

- 20 to 50 billion IoT devices by 2020
 - ❑ All Capable of being subverted
 - ❑ Zombie Apocalypse or a New Terminator movie



ISSA

Information Systems Security Association
International

www.issa.org

Michael F. Angelo – CRISC, CISSP
Chief Security Architect
Micro Focus | NetIQ Corporation
angelom@netiq.com

QUESTIONS?