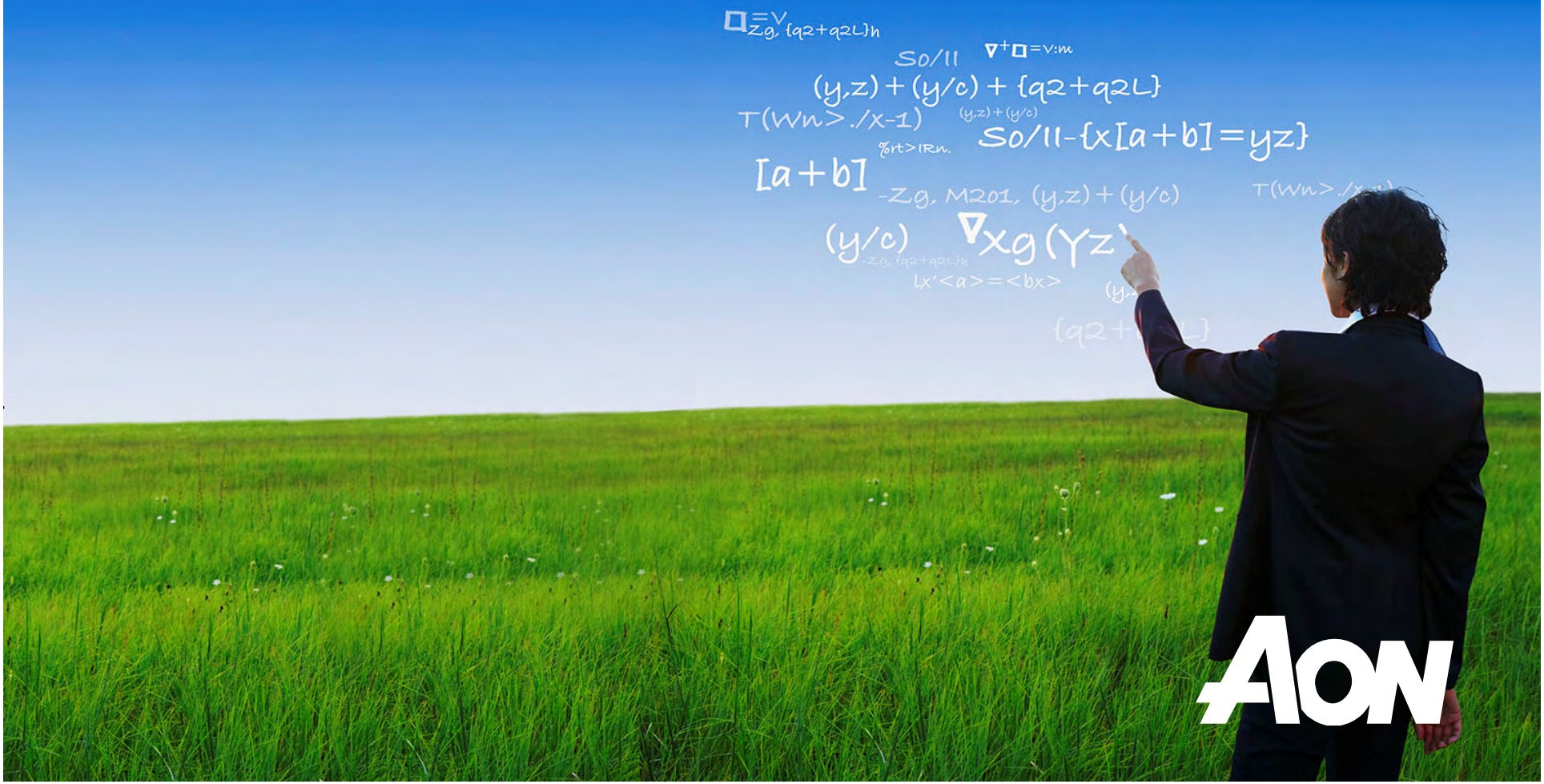
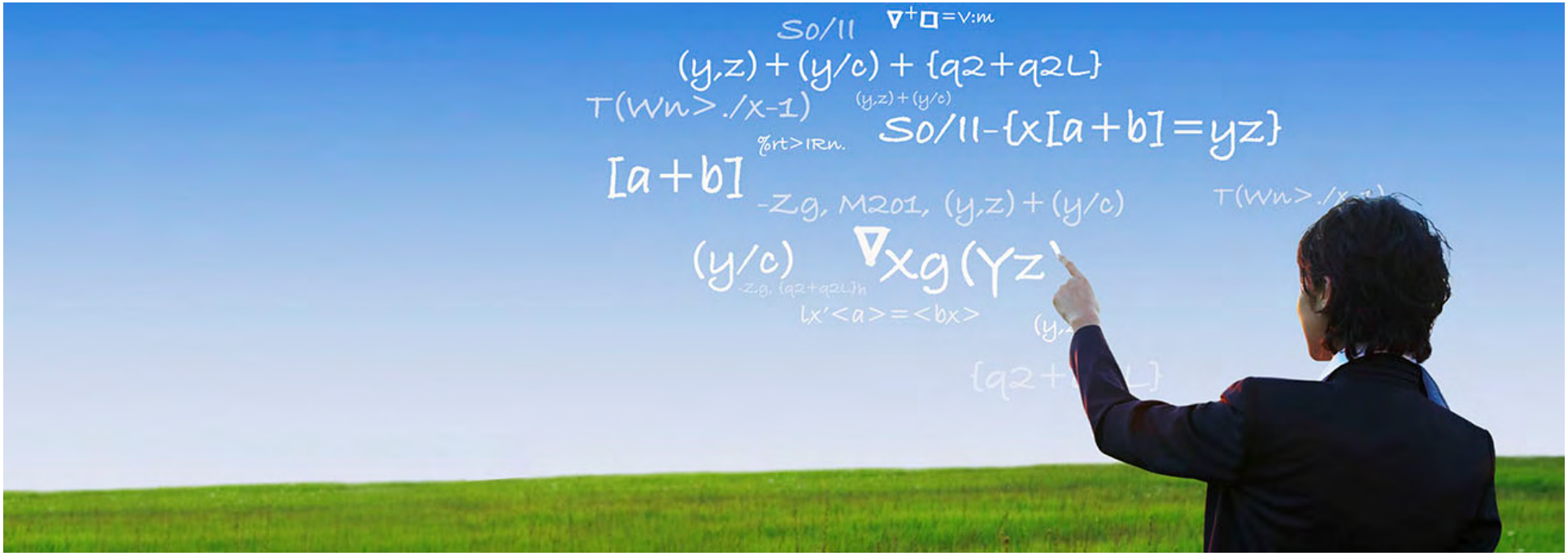
Cyber Risk Analytics

Southern California Casualty Actuarial Club

May 15th, 2014



Outline



What is Cyber Risk?

Table 1: Taxonomy of Operational Risk

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2 Deliberate		3.1.5 Information flow	4.1.5 Unrest
1.2.1 Fraud	**2.2 Software**	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.2 Sabotage	2.2.1 Compatibility	3.1.7 Service level agreements	
1.2.3 Theft	2.2.2 Configuration management	3.1.8 Task hand-off	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control		4.2.1 Regulatory compliance
	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3 Inaction	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.1 Skills	2.2.6 Testing	3.2.2 Metrics	
1.3.2 Knowledge		3.2.3 Periodic review	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.4 Process ownership	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design		4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	
	2.3.4 Complexity	3.3.2 Funding	**4.4 Service dependencies**
		3.3.3 Training and development	4.4.1 Utilities
		3.3.4 Procurement	4.4.2 Emergency services
			4.4.3 Fuel
			4.4.4 Transportation

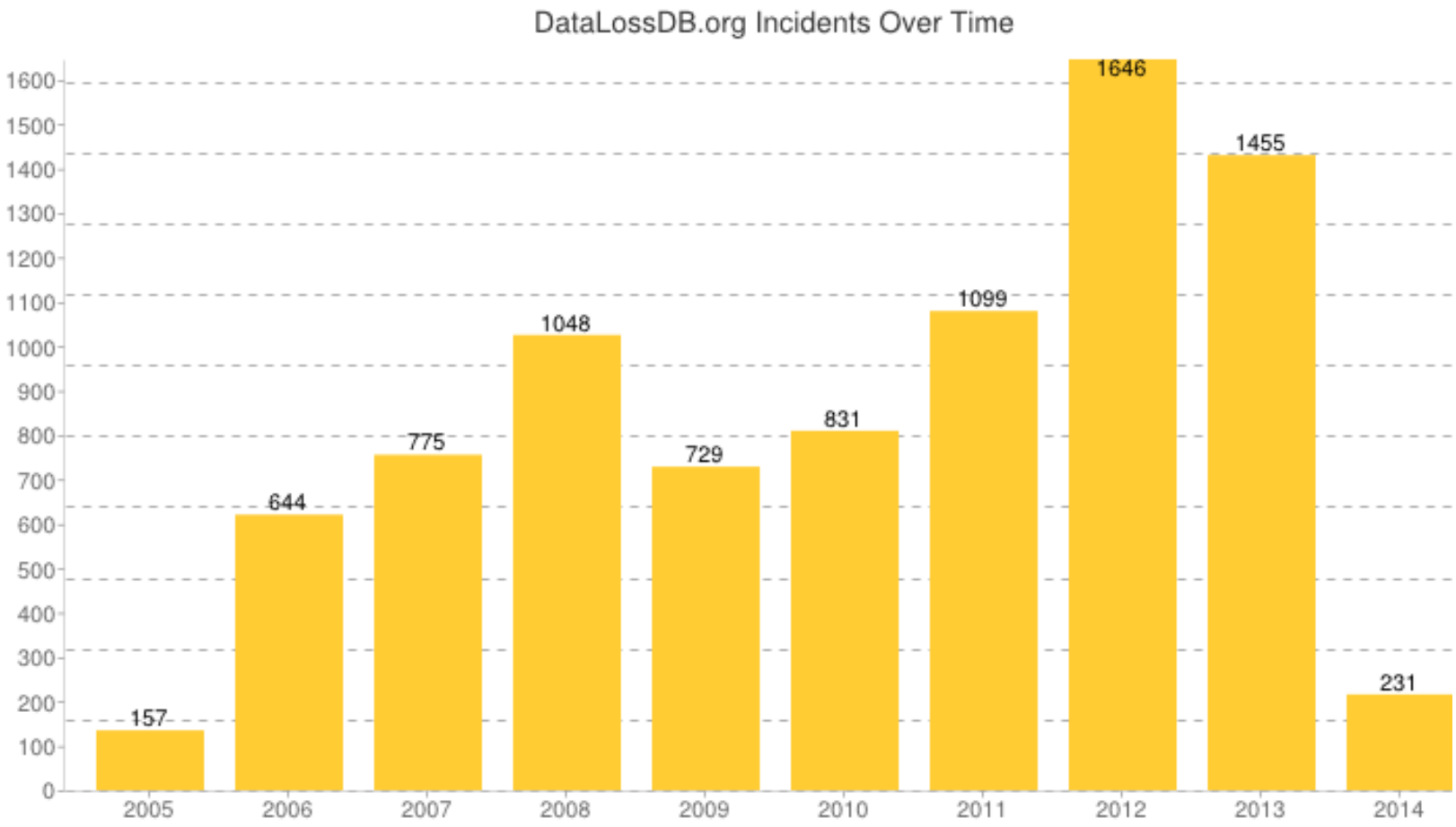
How is cyber risk defined in insurance?

- **Common 1st Party Insurance Coverage**
  - Investigation costs, crisis management, notification costs, credit monitoring, restoration of data resulting from
    - Theft of identities or private information
    - Unauthorized access to data/computer networks

- **Common 3rd Party Insurance Coverage**
  - Lawsuits and regulatory actions resulting from
    - A failure or violation of the security system
    - Theft of hardware
    - Failure to disclose a breach, under required breach laws

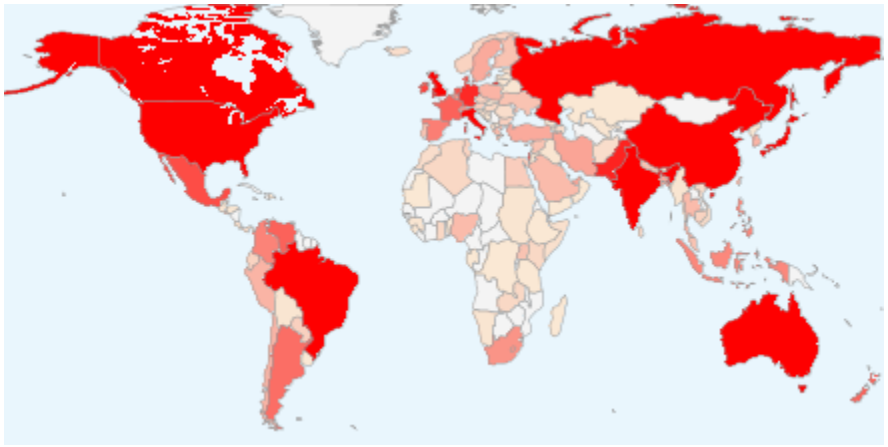
- **Other insurance or non-insured items:**
  - Revenue loss from cyber event (optional 1st party coverage)
  - Lost productivity or reputational damage
  - Internal costs , overhead, and physical damage to property
  - Data as an asset (intellectual property, trade secrets)

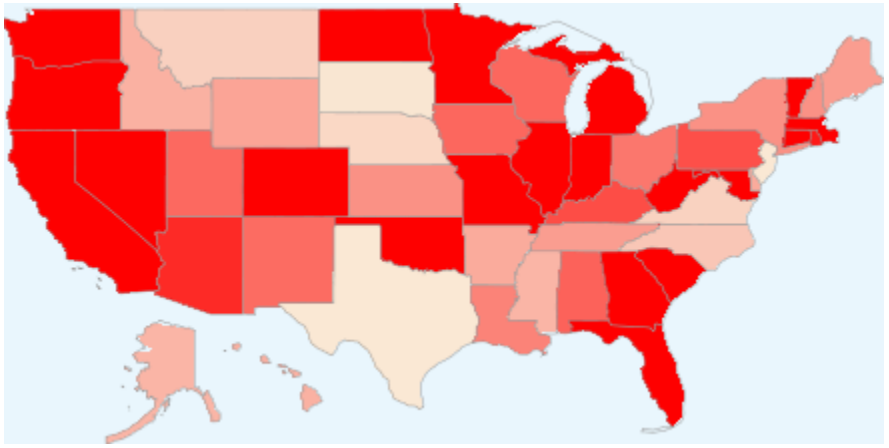
Current Trends - Incidents



* From DataLossDB.org website

Current Trends – Risk Maps





* From DataLossDB.org website

External Threat Actors*

	Organized Crime	State-Affiliated	Activists
Victim Industry	Finance, Retail, Food	Manufacturing, Professional, Transportation	Information, Public, Other
Region of operation	Eastern Europe, North America	East Asia (China)	Western Europe, North America
Desired Data	Payment cards, credentials, bank account info	Credentials, Trade Secrets, System Info	Personal info, Credentials, Internal data

* From Verizon 2013 Data Breach Investigations Report

High Profile Data Breaches 2012-2014

June 2012-Apr 2014
LinkedIn faces accusations of fraud in a class-action lawsuit stemming from a data breach its systems suffered almost two years ago. In June 2012, hackers infiltrated the professional networking site and posted passwords of 6.5 million LinkedIn members, and the plaintiff in the suit has claimed the site misrepresented its security measures. (encryption standards weaker than industry)

6.5M+ Records

Jan 2014-Apr 2014 Neiman Marcus confirmed that its database of customer information was hacked last month, around mid-December, the same time that Target stores were targeted

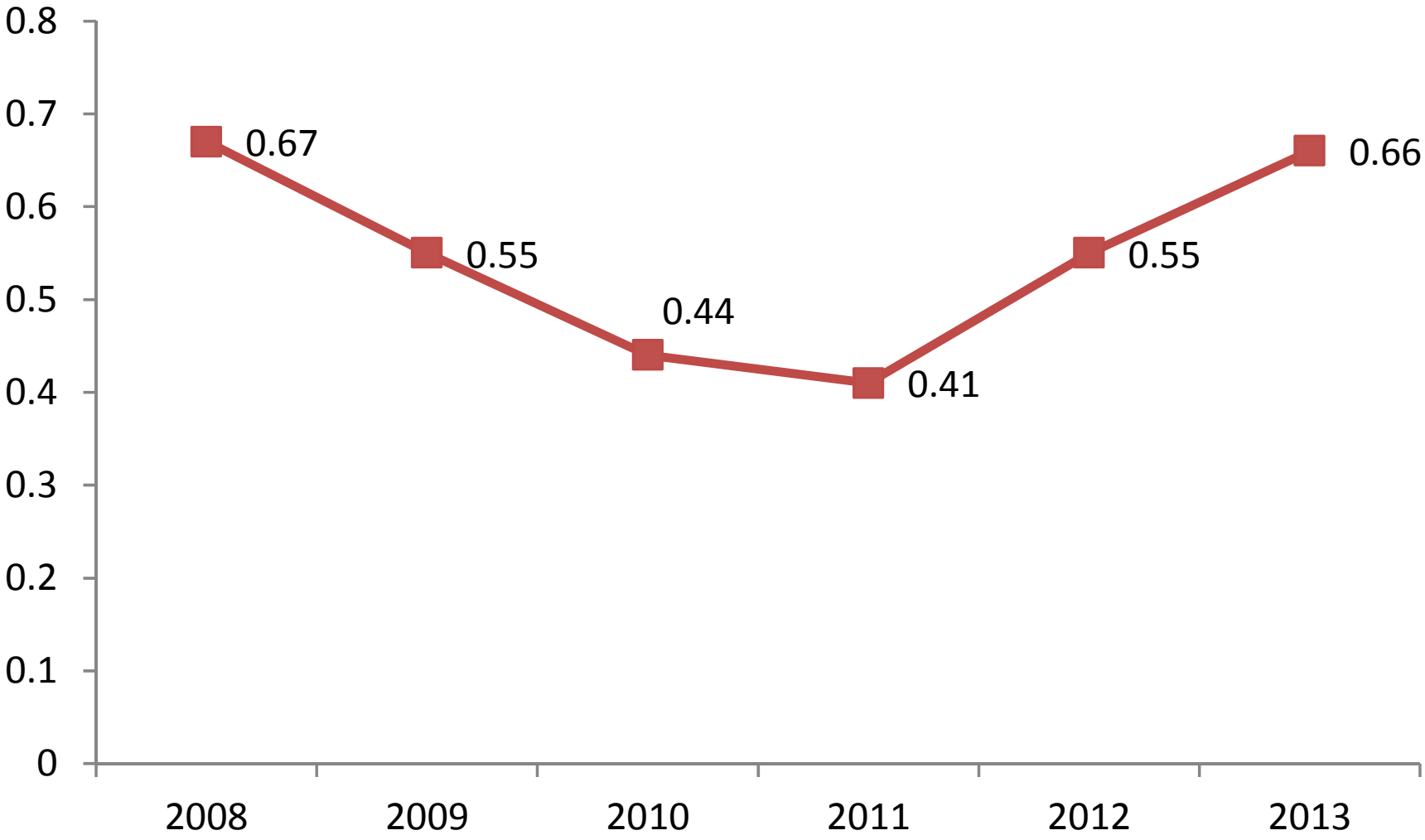
It has been reported that the breach at Neiman Marcus could as far back as July 2013 and that the breach was not fully contained until Sunday January 12, 2014.

1.1M+ Records

Dec 2013-Apr 2014 The data breach that exposed personal information of up to 70 million individuals has resulted in more than 80 lawsuits against the Minneapolis-based retailer, which revealed in December that malware on its checkout registers also led to the cyber theft of sensitive financial information from some 40 million credit and debit card accounts.

70M+ Records

Percent of breaches that remain undiscovered for months or more*



* From Verizon 2013 Data Breach Investigations Report

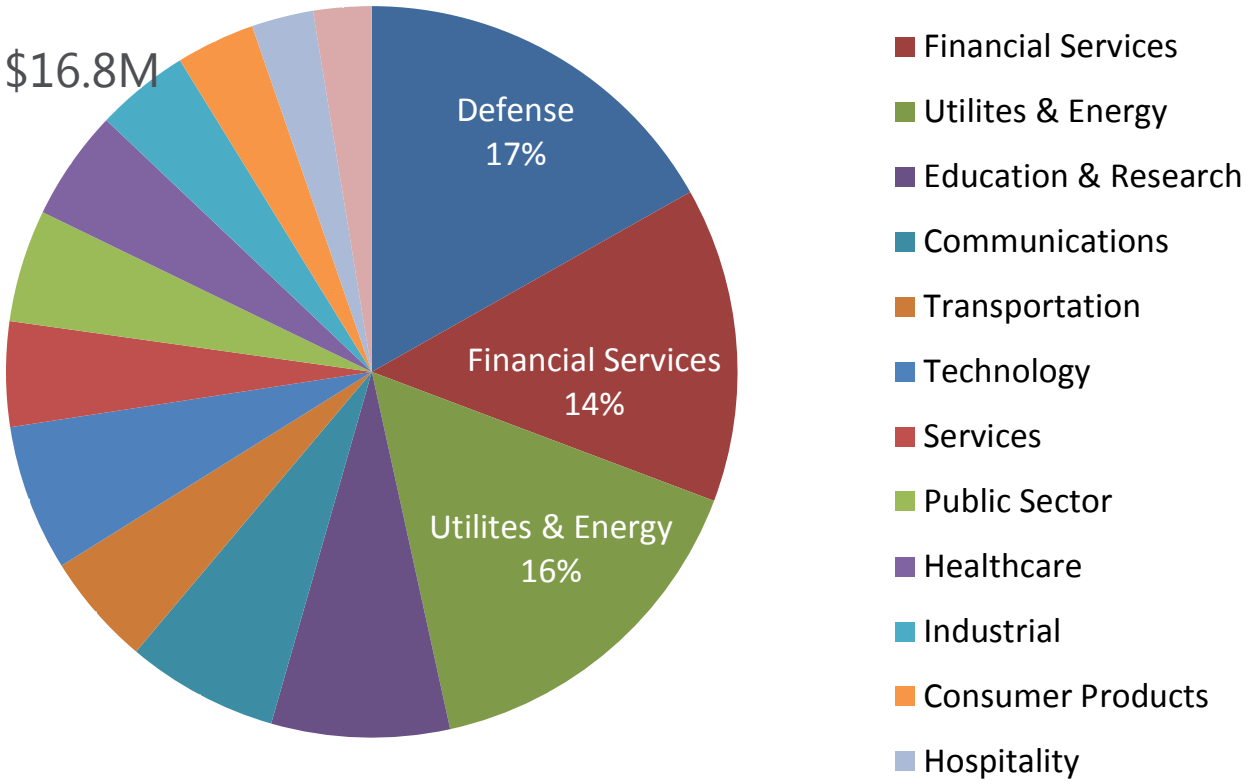
The Cyber Terrorism Threat

- **Oct 2013**- Defense Secretary **Leon E. Panetta** warned that the U.S. was facing the possibility of a **"cyber-Pearl Harbor"** and was increasingly vulnerable to foreign computer hackers. He warned "They could **derail passenger trains**, or even more dangerous, derail passengers trains loaded with **lethal chemicals**. They could **contaminate the water supply** in major cities, or **shut down the power grid** across large parts of the country."

Jan 2013 - U.S. Homeland Security Secretary **Janet Napolitano** warned that a major cyber attack is a looming threat and could have the same sort of impact as last year's Superstorm Sandy. Napolitano said a **"cyber 9/11"** could happen "imminently and that **critical infrastructure – including water, electricity, and gas** – was very vulnerable to such a strike.

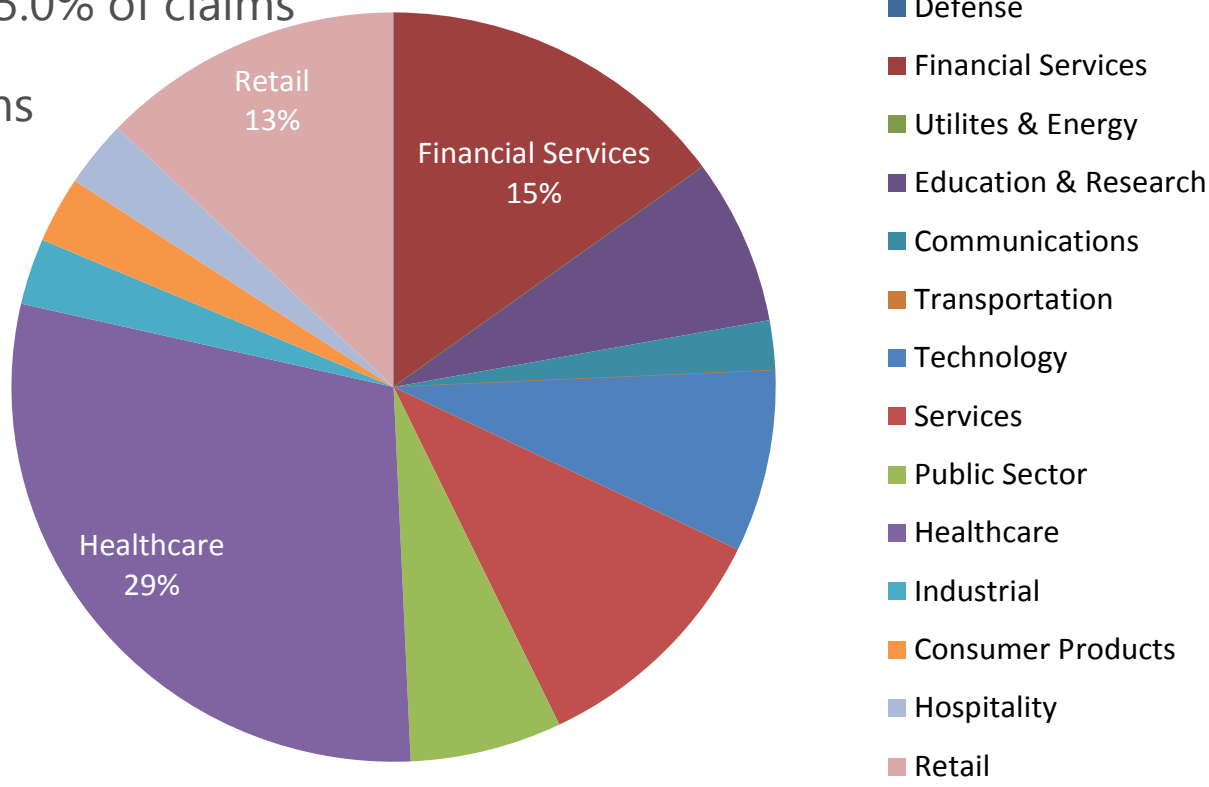
Which industries have been most impacted (non-insurance view)?

- According to the 2013 Cost of Cyber Crime Study by the Ponemon Institute, three industries have had the **highest average annualized cost of cyber crime** in the last three years. In 2013 the average annualized cost was:
  - **Defense**: $20.3M
  - **Utilities & Energy**: $19.1M
  - **Financial Services**: $16.8M



Which industries have been most impacted (insurance view)?

- According to the 2013 Cyber Liability & Data Breach Insurance Claim Study by NetDiligence, three industries have had the **highest number of claims** in the last three years. In 2013 the number of claims surveyed were:
  - **Healthcare**: 29.3% of claims
  - **Financial Services**: 15.0% of claims
  - **Retail:** 12.8% of claims



When should organizations be concerned about their cyber risk exposure?

- Organizations should be concerned about cyber risk if they:
  - Gather, maintain, disseminate or store **private information**
  - Have a high degree of **dependency on electronic processes** or computer networks
  - Engage vendors, independent contractors or **additional service providers**
  - Are subject to **regulatory statutes**
  - Are required to comply with PCI **Security Standards/Plastic Card Security statutes**
  - Are concerned about **contingent bodily injury and property damage** that may result from cyber incidents
  - Rely on or operate **critical infrastructure** (Personally Identifiable Information risks are less prominent for industries such as utilities, manufacturing and logistics)
  - Are concerned about intentional acts by **rogue employees**
  - Are a public company subject to the **SEC Cyber Disclosure Guidance of 2011**

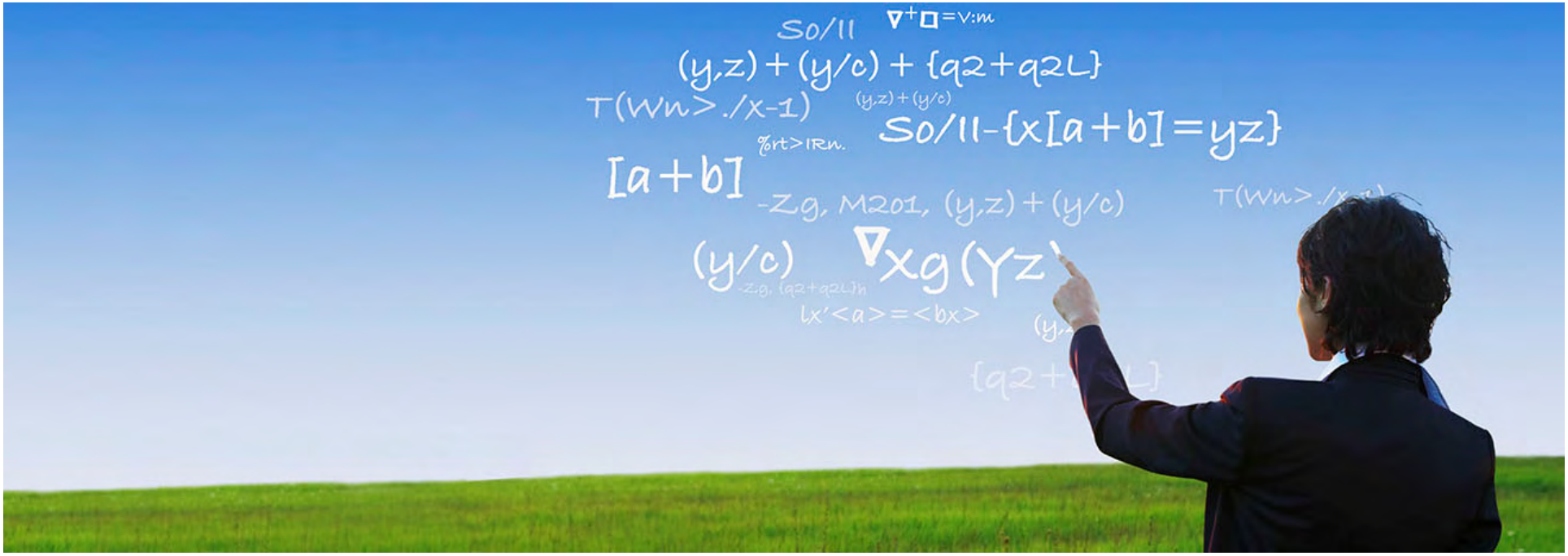
Banks


Defense


Cloud Computing Service Providers


Utilities


Technology



Cyber Risk - Risk Transfer & Mitigation

How do organizations mitigate or transfer cyber risk?

- Some exposures can be **transferred contractually** if outsourcing services. **Insurance solutions exist** if vendor will not take responsibility

- Marketplace evolving to provide **services solution**, including loss control resources, data breach coaches, dedicated claims resources, pre-approved panels of vendors and service providers to address each element of breach response

- More than 10 markets provide **cyber coverage on a primary basis**

- Numerous additional markets available for consideration of **excess limits**

Why aren't standard insurance policies enough?

- While existing forms sometimes carry a level of coverage, they were not intended to cover many risks associated with an increasingly digital world. Typical forms respond as follows:
  - **General Liability**: covers BI & PD, but **does not cover economic loss (loss of income or production).** May exclude cyber events.
  - **Errors & Omissions**: covers economic damages **resulting from a failure of defined services only**, and may contain **exclusions for data and privacy breaches**
  - **Property**: covers tangible property, which data is not. **Loss must be caused by a physical peril** while perils to data are more likely to be viruses or hackers
  - **Crime**: covers employees and generally only money, securities and tangible property. **No coverage for third party property** such as customer/client data

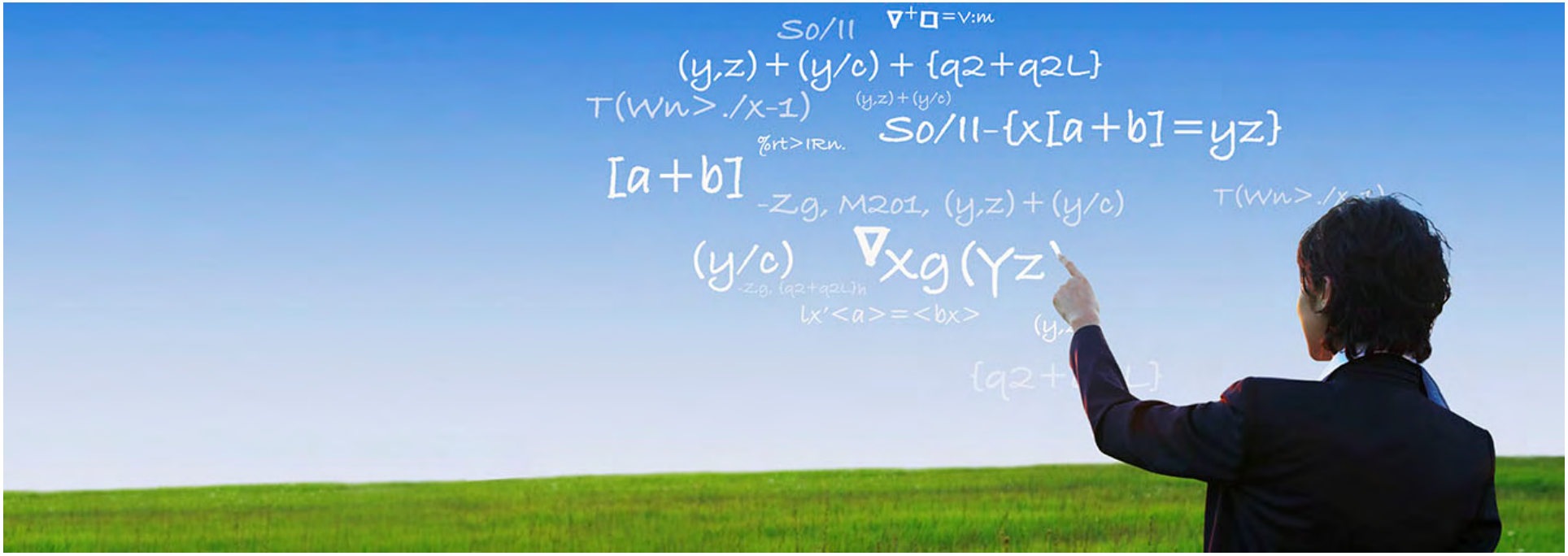
What is the scope of today's cyber coverage?

3rd Party Coverage

- Wrongful disclosure of Personally Identifiable Information, Protected Health Information or **confidential corporate information in the client's care, custody and control** via a computer network or off-line (e.g., via laptop, paper records, disks)
- **Failure of computer network security** to guard against threats such as hackers, viruses, worms, Trojan horses and denial-of-service attacks whether or not resulting from the provision of professional services
- Content liability perils such as **defamation and infringement of intellectual property rights** arising out of website, marketing and advertising activities
- Security or privacy breach regulatory proceedings (including associated **fines and penalties**)

1st Party Coverage

- **Network business interruption**: loss of income and extra expense due to network security failure
- **Intangible property**: costs to restore or recreate data or software resulting from network security failure
- Breach event **notification/management costs** associated with:
  - Statutory notification requirements, including the hiring of outside law firms and public relations consultants
  - Credit monitoring/protection
  - Notification hot line/call center
  - Forensic costs
  - Identity theft resources
- **Cyber extortion**



Cyber Risk Modeling

AON

Issues to address with cyber modeling

- What is the exposure to risk? (licenses, records, access points)
- Is there any internal data? (SIEM system is critical)
- How do you use external data (Various sources with many different views)
- How do you map data sources to insurance and limit of liability contracts?
- How do you address IT standards and process improvements? (SES Score)

One way to model cyber risk…

The Aon cyber model has the capability to quantify Data Breach & Security Failure Loss Exposures…

- Quantify the aggregate exposure to Cyber risk (1st and 3rd party) in any given quarter
- Quantify the exposure to any single event (Denial of Service, lost/stolen device…etc.)
- Quantify the exposure to any single customer contract and potentially price for it

Note: Loss per record is NOT effective cost estimator, as confirmed by NetDiligence insurance claim study

Cyber Data Industry Sources

- 2013 Ponemon Cost of Data Breach and Cost of Cyber Crime Studies
- 2013 Verizon Data Breach Investigations Report
- 2013 NetDiligence Cyber Liability & Data Breach Insurance Claims
- Recent Aon Proprietary Large Claim Settlements

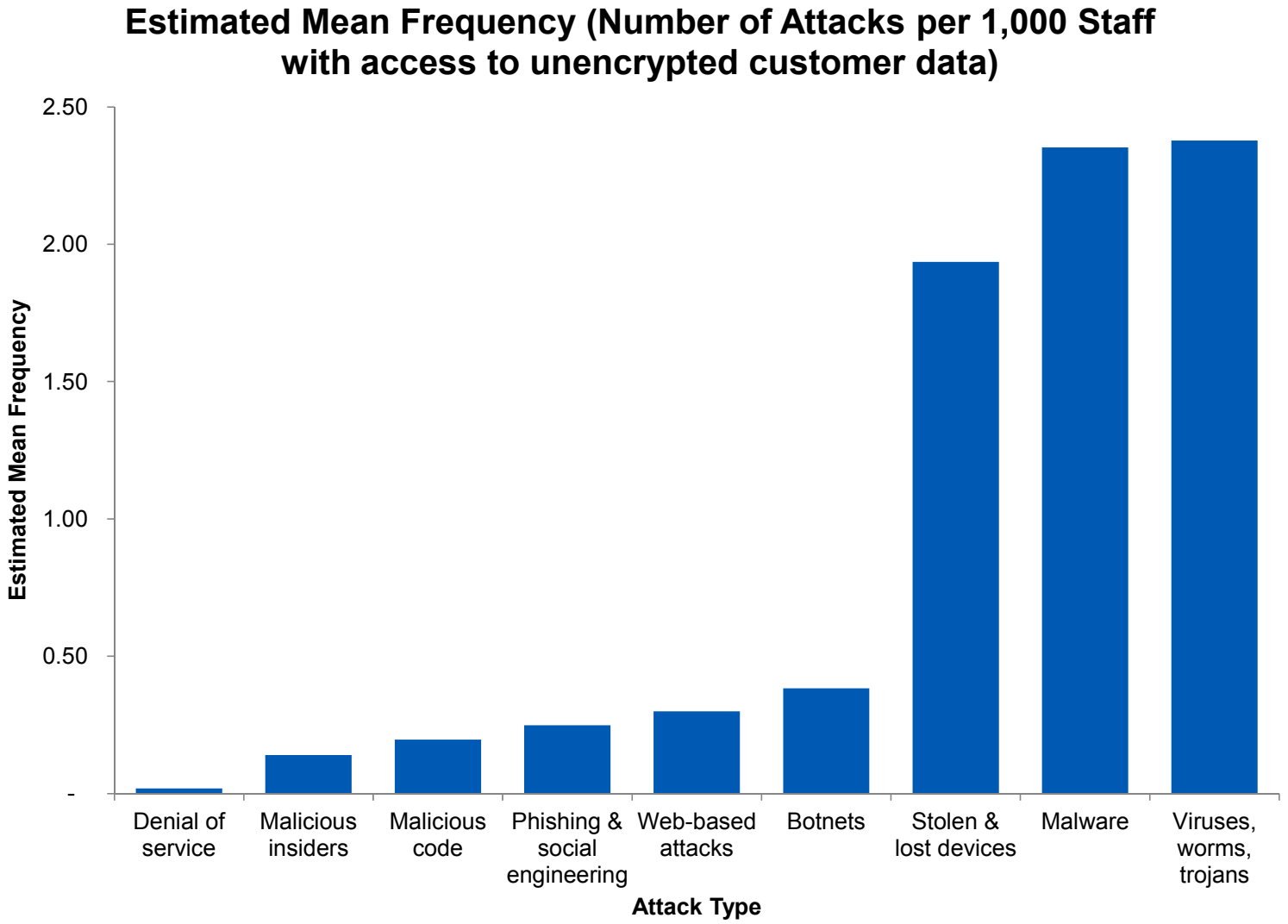
Summary of Key Industry Factors Used in Model

- Number of Enterprise Seats/Licenses/Encrypted access
- Number of Attacks Per Week
- Frequency Relativity by Attack Type
- Frequency Adjustment for Industry Mix
- Frequency Adjustment for Use of SIEM Technology
- Distribution of Cyber Crime Total Annualized Costs
- Distribution of Cyber Crime Internal & External Costs
- Distribution of Cyber Crime Internal Direct & Indirect Costs
- Distribution of Annualized Cyber Crime Costs by Attack Type
- Severity Adjustment for SES Score
- Frequency & Severity Trend
- Conversion Rate Incident to Loss

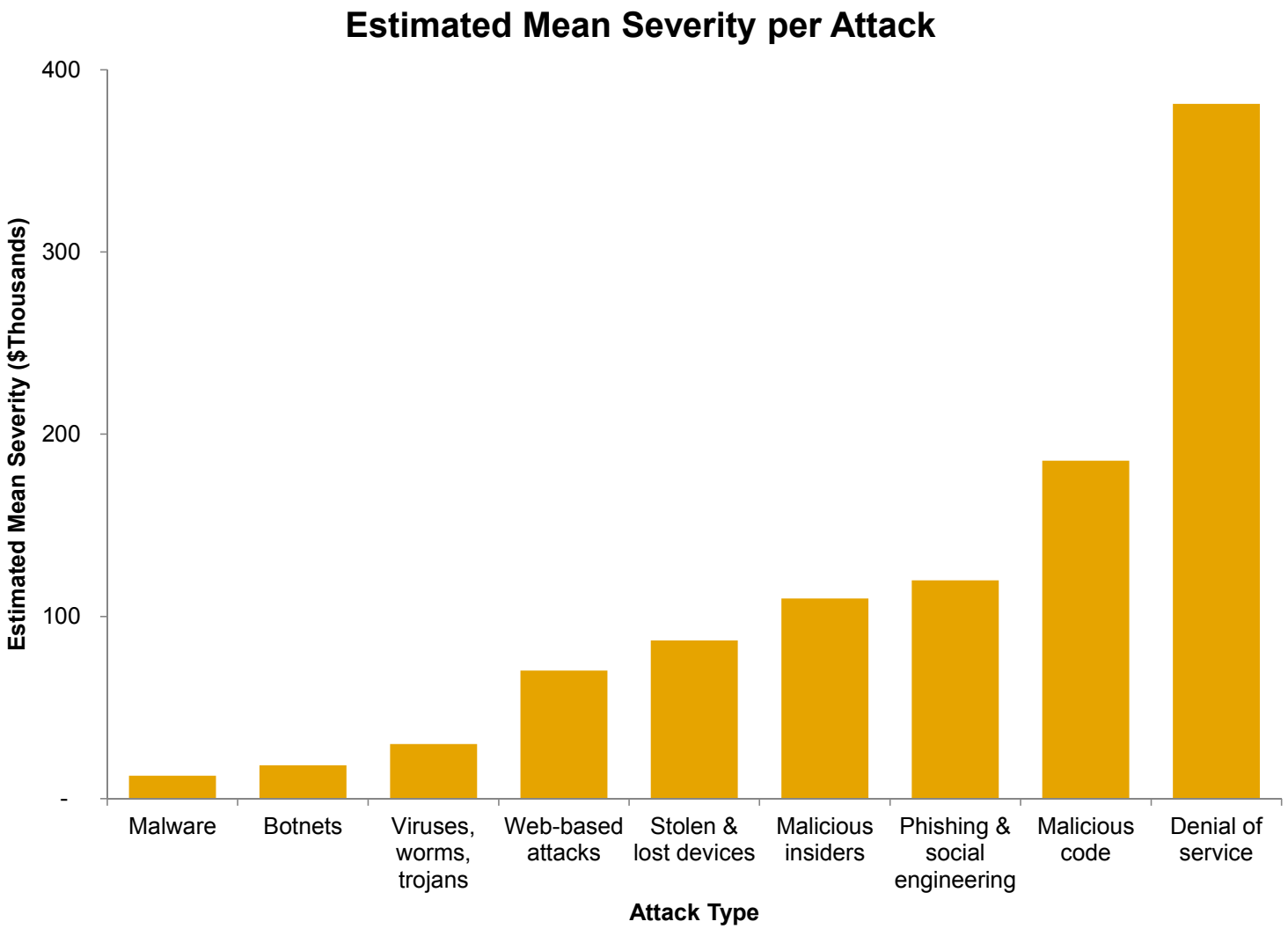
Losses included in modeling

Loss	Cyber Insurance	Included?
Investigation	1st Party	Yes
Crisis mangement	1st Party	Yes
Notification costs	1st Party	Yes
Credit monitoring	1st Party	Yes
Restoration of data	1st Party	Yes
Settlement/judgements	3rd Party	Yes
Defense costs	3rd Party	Yes
Punitive/multiple damages	3rd Party	Yes
Business Interruption	Special request	No
Internal labor costs	Not covered	No
Overhead	Not covered	No
Lost productivity	Not covered	No

Estimated Mean Frequency (λ)

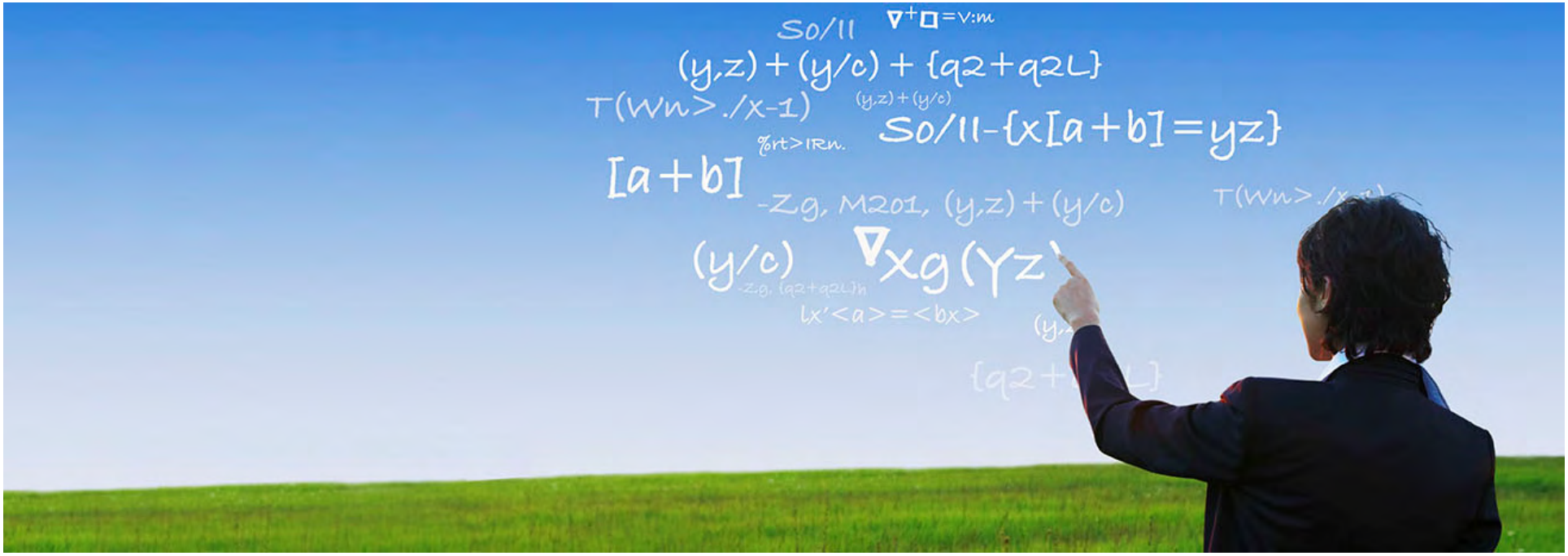


Estimated Mean Severity (μ)



Security Provisions that Modified Our Results

- SIEM (Security Incident and Event Management)
  - Reduced severity by 20%
- SES (Security Effectiveness Score)
  - Reduced frequency by 10%
- Encryption technology and key access
  - Reduced frequency by 20%
- Contract language
  - Reduced severity by 20%



Case Study:

Cyber Risk Model Structure

Frequency Model

Frequency

Industry Attacks/ 1,000 Enterprise Seats

20% Conversion Rate Incident > Dollar Loss

Industry:

Client frequency 6.5% **higher** due to customer industry mix

SIEM :

Client frequency 20% **lower** due to use of SIEM technologies

Severity Model

Severity per Attack

Industry Severity Mean

Industry Severity Standard Deviation

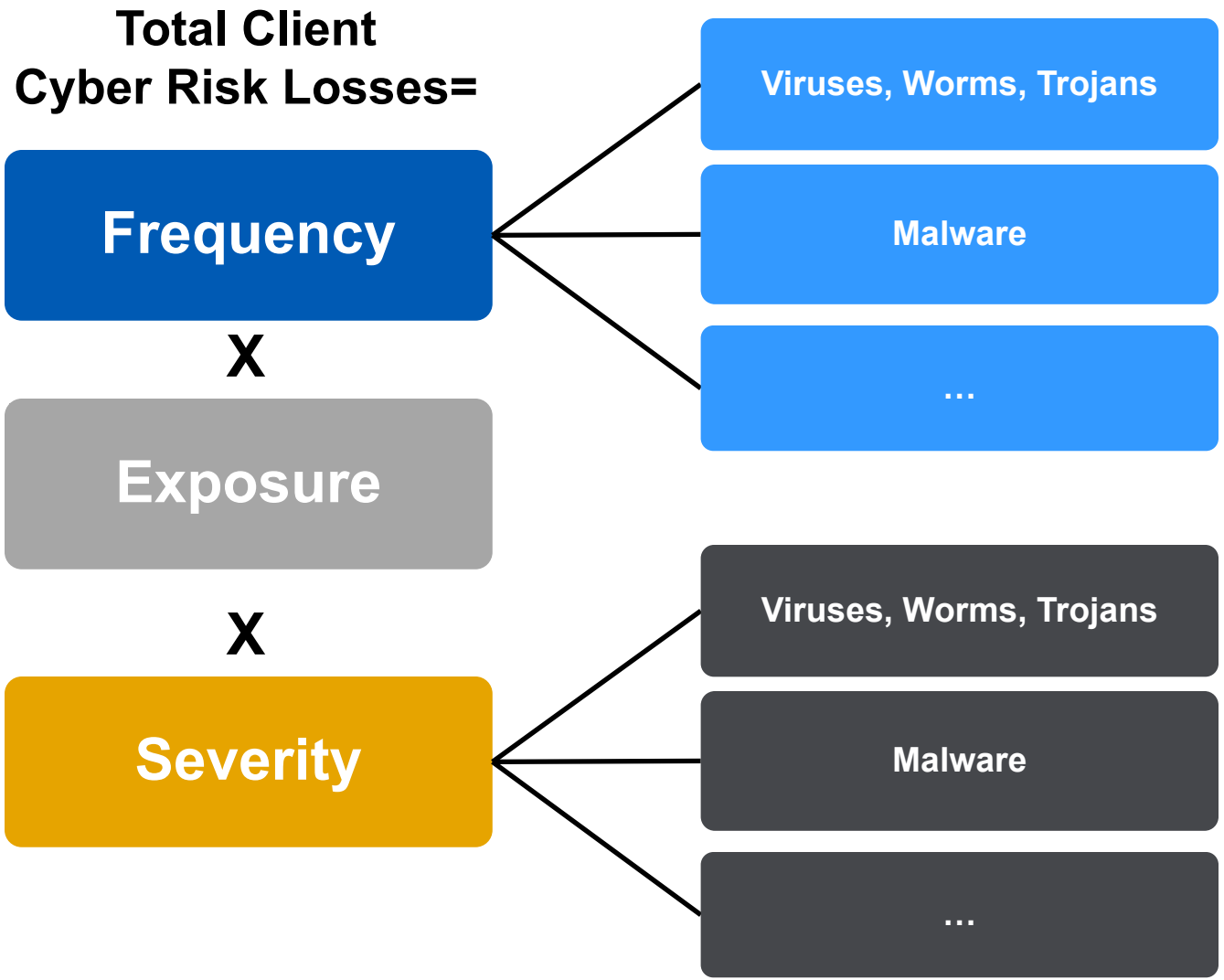
SES:

Client severity 25% **lower** due to security posture

Encryption:

Client **Stolen & Lost Devices Only** severity **5.0% lower** due to encryption standards

Cyber Risk Model Build– High Level

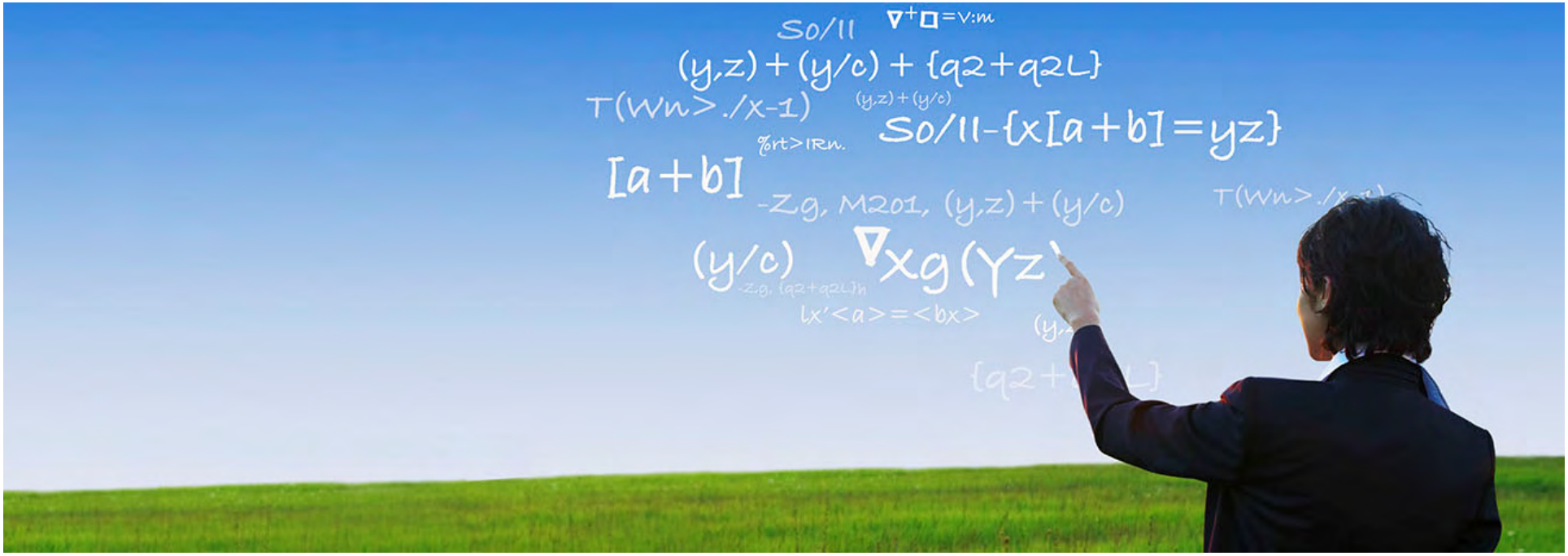


Frequency = Number of Attacks per unit of Exposure

Exposure = number of staff w/ unencrypted access to customer data

Severity = Average Size of Loss per Attack

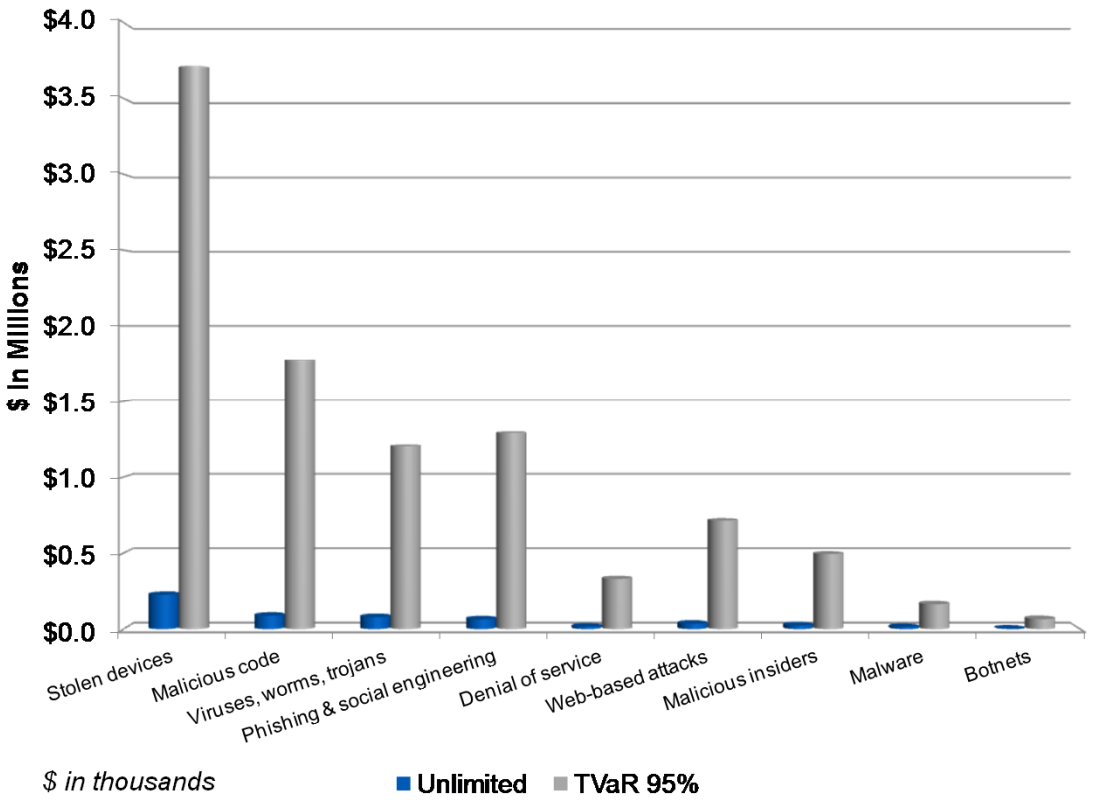
Attack Types:
-Viruses, worms, trojans
-Malware
-Stolen & lost devices
-Botnets
-Web-based attacks
-Phishing & social engineering
-Malicious code
-Malicious insiders
-Denial of service



Case Study:

Cyber Risk Modeling Results

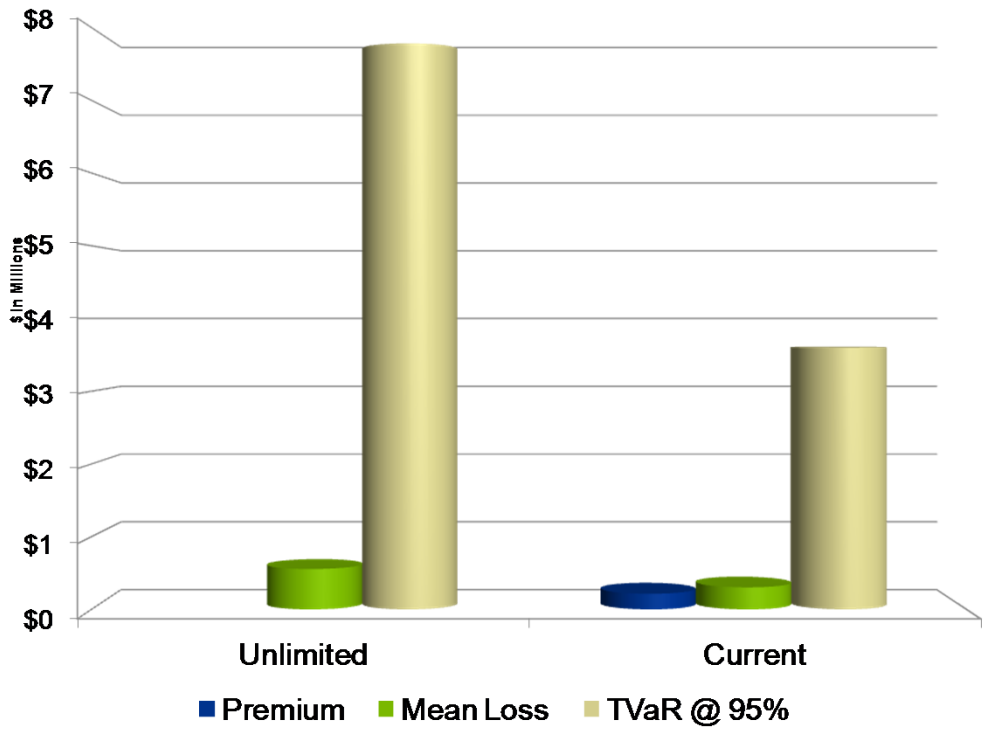
Unlimited Losses by Attack Type



- Viruses/worms/trojans and malware have the highest estimated frequencies, but have the 3rd lowest, and lowest severities, respectively
- Denial of service and malicious code have the lowest and 3rd lowest frequencies, but have the top 2 severities
- Stolen & lost devices represent the largest exposure because they have the 3rd highest frequency and the 5th highest severity

Criteria	Viruses, worms, trojans	Malware	Botnets	Web-based attacks	Stolen & lost devices	Malicious code	Malicious insiders	Phishing & social engineer-ing	Denial of service
Mean Losses	$ 90.0	$ 15.0	$ 5.0	$ 40.0	$ 350.0	$ 90.0	$ 25.0	$ 70.0	$ 20.0
TVaR @ 95%	$ 1,250.0	$ 250.0	$ 75.0	$ 750.0	$ 3,750.0	$ 1,990.0	$ 500.0	$ 1,400.0	$ 350.0

Current Program Analysis



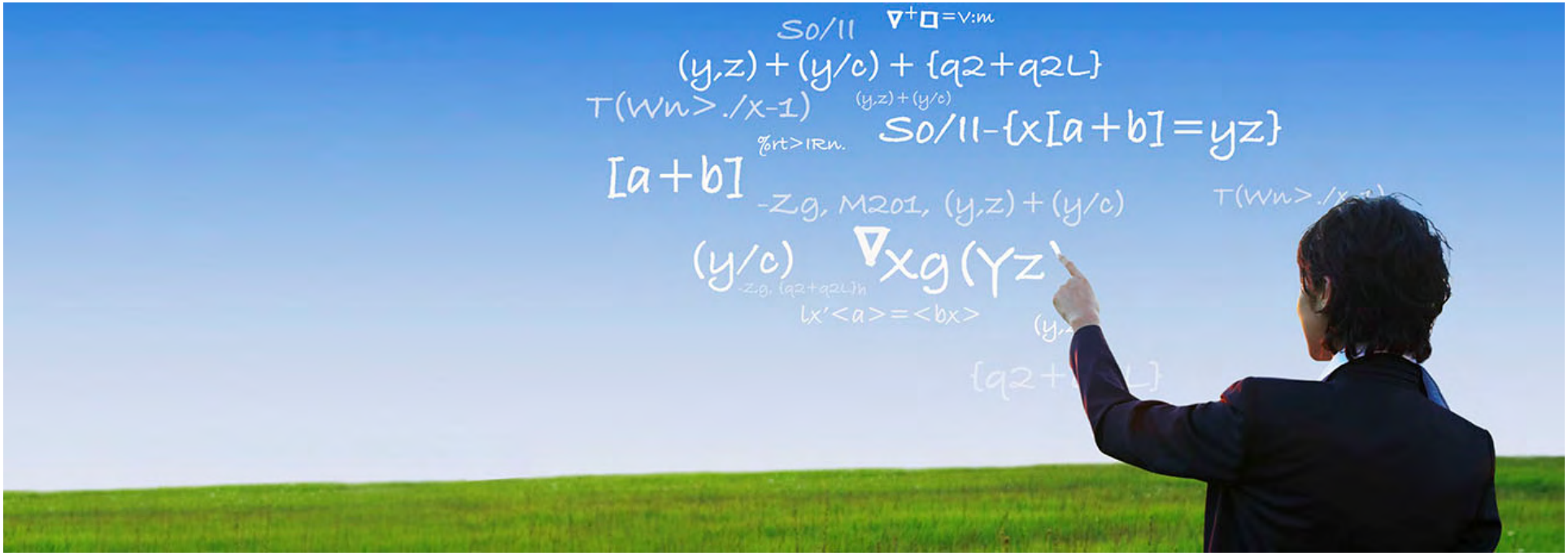
$ in millions

Criteria	Unlimited Loss	Current Program
Mean Losses	$575,000	$300,000
Estimated Premium		$250,000
Mean TCOR	$575,000	$500,000
TVaR @ 95%	$8,000,000	$5,000,000

- The Current Program provides catastrophic loss protection
  - Compared to purchasing no insurance (Unlimited Loss), the Current Program provides catastrophic loss protection of $5.0 million as measured by TVaR at the 95th percentile, and it results in a Mean TCOR decrease of $75,000
    - Current Program does a good job of lowering both the Mean TCOR and TVaR @ 95%

Case Study Conclusions

- Client has significant exposure to cyber risk
- Stolen/lost devices and denial of service attacks are the single largest sources of risk to the organization
- Current insurance limit of $XXM is very modest compared to the overall risk to the organization. Additional risk transfer methods should be considered.
- Security measures and controls are some of the best in the industry, but cyber risk continues to exist through potential break-downs in those controls
- It is important for the organization to measure this risk and make a conscious decision on the appropriate level of risk for Client



Conclusions

Conclusions

- Cyber crimes have become common occurrences and continue to be costly to organizations
- Actuaries can help quantify cyber risk through the use of stochastic modeling and available industry data
- Industry information is critical and evolving
- Insurance contracts are developing

Aon Contact List

Loren Nickel, FCAS, CFA, MAAA
Regional Director & Actuary
Actuarial & Analytics
+1.415.486.7369
loren.nickel@aon.com

Conditions and Limitations

Inherent Uncertainty

Actuarial calculations produce estimates of inherently uncertain future contingent events. We believe that the estimates provided represent reasonable provisions based on the appropriate application of actuarial techniques to the available data. However, there is no guarantee that actual future losses will not differ from the estimates included herein. This is especially true for analyses of losses in layers above the level for which client data alone is of sufficient volume and stability to be predictive of exposure to loss. In that situation, we have supplemented client data with relevant data from other sources and consequently our estimates are subject to a greater degree of uncertainty than would be expected if we were able to rely on client data alone.

Data Reliance

In conducting this analysis, we relied upon the provided data without audit or independent verification; however, we reviewed it for reasonableness and consistency. Any inaccuracies in quantitative data or qualitative representations could have a significant effect on the results of our analysis.

Use and Distribution

Use of this report is limited to the specific purpose described in the Introduction section. Other uses are prohibited without an executed release with Aon.

Actuarial Standards of Practice

The actuarial component of this analysis was performed by Members of the Casualty Actuarial Society and Members of the American Academy of Actuaries, who meet the Qualification Standards of the American Academy of Actuaries to provide the actuarial work product contained herein. We performed this analysis using generally accepted actuarial principles and in accordance with all relevant Actuarial Standards of Practice.

Appendix

SES Score

APPENDIX 3: 24 SECURITY EFFECTIVENESS SCORE (SES) ITEMS

The following table summarizes the average SES by item for 46 benchmarked companies.

Security effectiveness scoring attributions	Item score
Determine the root cause of data loss or theft	0.20
Identity all significant data breach incidents	0.27
Know where sensitive or confidential information is physically located	-0.48
Secure sensitive or confidential data at rest	-0.02
Secure sensitive or confidential data in motion	-0.57
Secure endpoints to the network	0.40
Identify and authenticate end-users before granting access to confidential information	0.42
Protect sensitive or confidential information used by outsourcers	1.05
Prevent or curtail the theft of information assets	0.19
Prevent or curtail external penetration or hacking attempts	0.02
Limit physical access to devices containing sensitive or confidential information	-0.15
Measure the effectiveness of security program components	-0.38
Ensure minimal downtime or disruptions to systems resulting from security issues	0.61
Test (prove) compliance with legal and regulatory requirements	-0.94
Test (prove) compliance with self-regulatory mandates	1.53
Prevent or curtail viruses, malware and spyware infections	-0.01
Ensure security patches are updated in a timely and comprehensive fashion	-0.48
Control all live data used in systems development activities	-0.14
Monitor and strictly enforce security policies	0.57
Attract and retain professional security personnel	1.62
Training and awareness program for all users	-0.16
Conduct audits or assessments on an ongoing basis	1.08
Ensure security program is consistently managed	-0.06
Prevent or curtail denial of service attacks	0.19
Monitor networks, systems and logs for unusual events	-0.14
Average security effectiveness score	**0.18**

Appendix 2 – PCI DSS

What is PCI?
A: The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that **process, store** or **transmit** credit card information maintain a secure environment. Essentially any merchant that has a Merchant ID (MID).
The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).
It is important to note, the payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

To whom does PCI apply?
A: PCI applies to ALL organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. Said another way, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

PCI DSS 3.0 was published Nov 2013

Appendix 3 – ISO Standards

ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is *ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements*. As of July 2013[update], a new version is in draft: ISO/IEC 27001:2013. ISO 27001:2013 has been available in its release form since 25 September 2013.

ISO/IEC 27001:2005 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

The standard contains 11 domains (apart from introductory sections):

- Security policy - management direction
- Organization of information security - governance of information security
- Asset management - inventory and classification of information assets
- Human resources security - security aspects for employees joining, moving and leaving an organization
- Physical and environmental security - protection of the computer facilities
- Communications and operations management - management of technical security controls in systems and networks
- Access control - restriction of access rights to networks, systems, applications, functions and data
- Information systems acquisition, development and maintenance - building security into applications
- Information security incident management - anticipating and responding appropriately to information security breaches
- Business continuity management - protecting, maintaining and recovering business-critical processes and systems
- Compliance - ensuring conformance with information security policies, standards, laws and regulations

Appendix 4 - Encryption Standards

FIPS 46-3, Data Encryption Standard (DES). FIPS 46-3 specifies the DES algorithm. It was originally adopted in 1977 as FIPS 46, and reaffirmed in 1983 and 1987 as FIPS 46-1 and FIPS 46-2 with changes to the allowed embodiment of the algorithm. In 1999, the standard was affirmed as FIPS 46-3, adopting the Triple DES algorithm (TDES) as specified in the American National Standards Institute (ANSI) X9.52 standard, and continuing to allow [single] DES for legacy systems, as specified in FIPS 46-2. ***When FIPS 46-3 comes up for review in 2004, single DES will no longer be approved for Federal Government applications***. Therefore, neither new applications nor current legacy systems, including systems using cryptographic modules previously validated against FIPS 140-1 and 2, will be approved for using single DES after 2004. However, TDES and AES (the algorithm specified in FIPS 197; see below) will continue to be approved for all systems. Agencies should develop and implement a transition plan for using approved algorithms other than single DES.

TDES is a method for encrypting data in 64-bit blocks using three 56-bit keys by combining three successive invocations of the DES algorithm. ANSI X9.52 specifies seven modes of operation for TDES and three keying options: 1) the three keys may be identical (one key TDES), 2) the first and third key may be the same but different from the second key (two key TDES), or 3) all three keys may be different (three key TDES). One key TDES is equivalent to DES under the same key; therefore, one key TDES, like DES, is currently allowed only for legacy systems, but will not be approved after 2004. Two key TDES provides more security than one key TDES (or DES), and three key TDES achieves the highest level of security for TDES. ***NIST recommends the use of three different 56-bit keys in Triple DES for Federal Government sensitive/unclassified applications.***

FIPS 197, Advanced Encryption Standard (AES). The encryption algorithm specified in FIPS 197 is the result of a multiyear, worldwide competition to develop a replacement algorithm for DES. The winning algorithm (originally known as Rijndael, but hereafter referred to as the AES algorithm) was announced in 2000 and adopted in FIPS 197 in 2001. The AES algorithm encrypts and decrypts data in 128-bit blocks, with three possible key sizes: 128, 192, or 256 bits. The nomenclature for the AES algorithm for the different key sizes is AES-x, where x is the size of the AES key. ***NIST considers all three AES key sizes adequate for Federal Government sensitive/unclassified applications***

Appendix 5 - SIEM

Security Information Event Management is normally referred to as SIEM and is typically a collection of two technologies, Security Information Management (SIM) and Security Event Management (SEM).
Security Information Management is also often referred to as Log Management, with Security Event Management often referred to as the Correlation Engine portion of SIEM.

The Log Management layer should be able to collect accounting and audit logs at large volumes, where as the Correlation Engine should be able to analysis the logs, picking out important behaviours and flagging them for review via alerts.

It is unusual, but not unheard of for vendors to only provide one of the solutions, either SIM or SEM, to the market, for example, Splunk and LogLogic are known as having strong SIM capability but poor SEM capability and Arcsight and RSA have strong SEM capability but poor SIM capability. All these vendors added extra capabilities in an attempt to address their weakness. It might be worth going for a product that has strong capabilities across both SIM and SEM, sign-up for our Webcast (below) for some recommendations from independent experts.

The problem with any SIEM solution is that it will collect logs from across the enterprise, millions of them! If you are collecting these logs, you are likely to want to look at them, and that is where the problem lies.

There is no doubt log analysis improves your risk profile. In fact the Data Breach Report from Verizon clearly states that in over 90% of the cases they investigated over the last five years, evidence of your breach was in the log file. If someone was conducting a thorough analysis of the logs at the time of the breach the breach would have been detected and could have been shut down.

It is therefore critical that any SIEM solution your are looking for has the capability to find "behaviours", rather than single events and just as important that creating the behavioural rules is easy and intuitive, not requiring vendor support to do so, as your team will be creating a number of them on an ongoing basis.