
BEA
BREACH EDUCATION ALLIANCE

Breach Education Alliance:
Integrated Team Approach With Complementary Resources

Best Practices; Retrospect from a Breach Investigation

Parameter Security

Goals of a Successful Investigation

Did an incident Occur?

Scope of Incident

Cause of Incident

Assess Damages

Activate BC/DR?

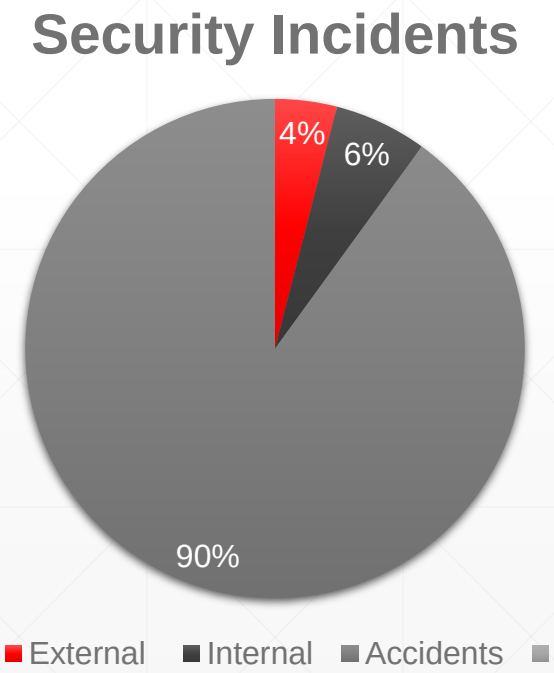
Consider further Actions

Not all Malicious

Malicious Attackers

50% - 60% are internal attackers

Malicious Attacks less than 10% of all security incidents



Goals of a successful Investigation

Did an incident Occur?

- Lack of Baseline
- Lack of Corporate Policies
- False-Positives

Scope of the Investigation

- Does it affect Confidentiality, Integrity, Availability?
- Is disclosure required?
- Will 3rd parties aid in the investigation?

Goals of a successful Investigation

Determine Cause

- Was the cause internal or External?
- Did a person cause it?
- Was it Malicious?

Assess Damage

- How does the incident affect Business Operations?
- Will the investigation affect Operations
- Will Business Operations impede the Investigation / Destroy Evidence

Goals of a successful Investigation

Activate BC/DR

- Did the incident inhibit/Cease Operations?
- Has the Integrity of data been compromised?
- Has your TCB been Compromised?

Further Actions

- Take Legal Action
- Report Incident to 3rd Party
- File an Insurance Claim
- Learn from the incident and plan


Best
Practices

Lack of knowledge of Environment

The most common mistake

- How can you identify malicious activity, if you don’t know what legitimate activity looks like?
- Inventory software, devices and other assets.
- Software updates often fix security problems, so download updates as soon as they become available.

Use strong Passwords or Password Phrases

- “Mary had a little lamb”.
  The space bar is a unique character!

- Easy to remember, don’t have to write them down and unique to everyone!

Train your employees …

- They need to be aware of Phishing and email traps, links, downloads.
- Security Awareness training is critical.

Understand your business…

- Key areas:
- Where are you vulnerable? What IP does your company have?
- What threats should you be aware of?
- What impact would these threats have on your business?
- What does potential Regulatory Compliance require of you?
- Establish risk thresholds or tolerance levels. Will you Mitigate, Accept or Insure those risks.

Questions / Contact Information:

John Poole

Parameter Security

Penetration Assessments | Forensics/IR | Compliance Assessments | Instruction

www.ParameterSecurity.com

John.Poole@ParameterSecurity.com

Direct: 314.442.0472 x503 | Mobile: 636.579.4393

cybersecurity/data breach/privacy™

Complex Issues – Here to Stay

CyberGroup/cybersecurity/data breach/privacy™

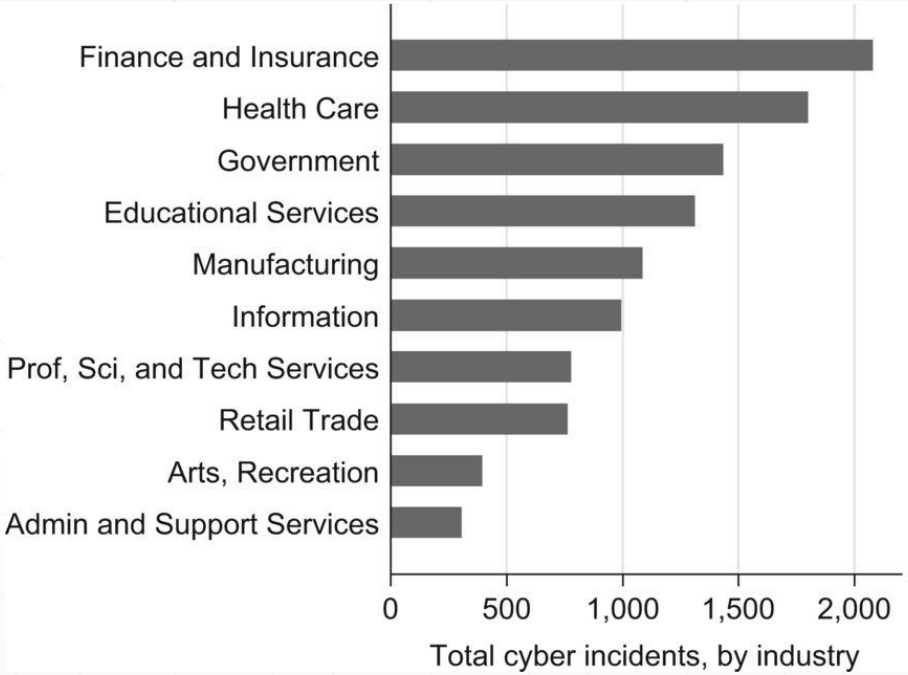
HEPLERBROOM LLC

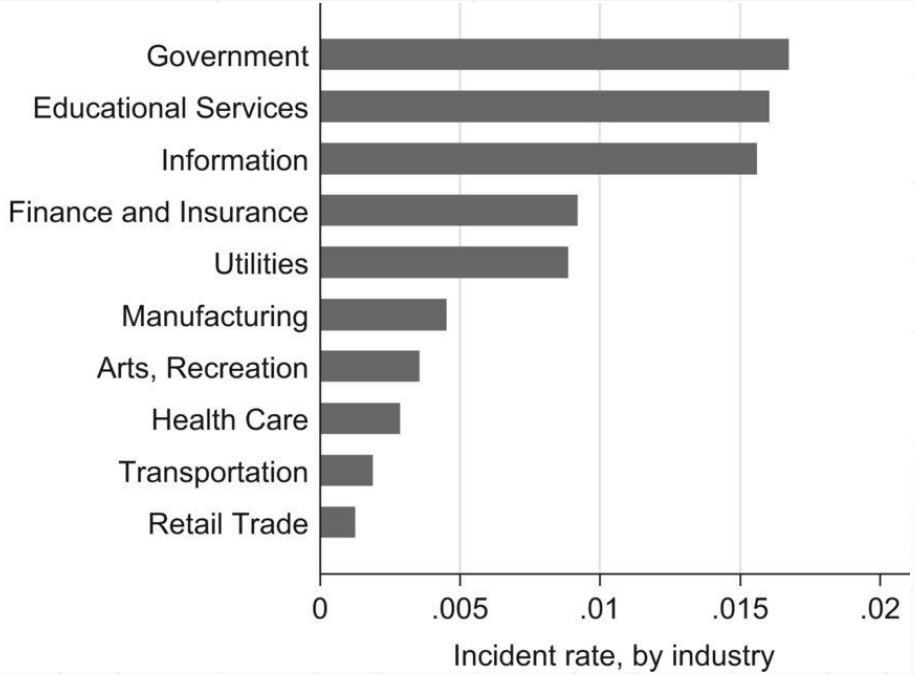
PROVEN LAWYERS IN THE RIGHT PLACES

Complex Issues — Here to Stay

- Sophisticated Threats, Evolving Technology, Internet of Things
- 64% increase—information security incidents 2015 vs 2014
- Healthcare—frequently attacked industry
  - Ransomware attacks
  - 100 million healthcare records compromised 2015 (credit card, email, SSN, employment, med history data)
  - High price on black market “dark internet”
  - Cyber thieves use data to launch spear phishing attacks, commit fraud, steal medical identities
- But no industry immune—
  - Manufacturing (automotive. chemical. corp. IP networks)
  - Financial Services (consumer banking, mobile apps)
  - Government (IRS and HHS breaches)
  - Transportation (freight, shipping, air)
  - Retail/Wholesale

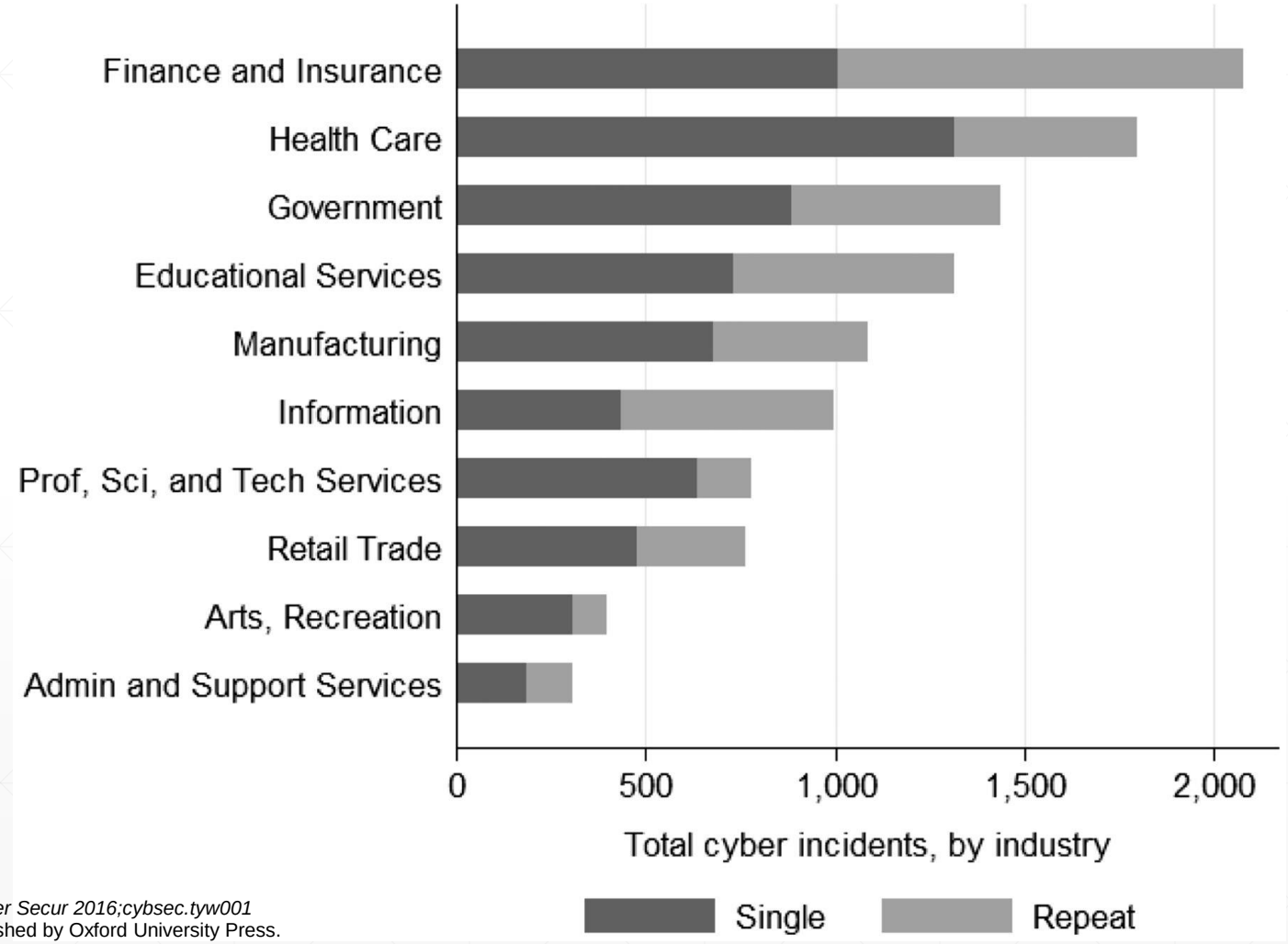
Cyber incidents, and rates, by industry





Sasha Romanosky J Cyber Secur 2016;cybsec.tyw001
© The Author 2016. Published by Oxford University Press.

Repeat incidents by industry.



Sasha Romanosky J Cyber Secur 2016;cybsec.tyw001
© The Author 2016. Published by Oxford University Press.

Costs

- Assessing/predicting costs of data breaches DIFFICULT--lack of quality data.
- High INTEREST AMONG firms at risk, insurance carriers, researchers, and social planners.
- Based on recent survey data estimates the average cost of a data breach is around $6.5 million (or, $217 per record; Ponemon 2015).
- Averages may be misleading: the statistical mean as a measure of the cost of a data breach (or cyber event) pegs the loss for a data breach at almost $6 million, but the median loss is only $170k.
- Similarly skewed values arise for phishing and security incidents.
- Privacy violations, however, account for a much larger median loss of $1.3 million.

Statistics Do Not Account For:

- Business interruption
- Reputational loss
- Customer retention/loss
- Cost of allocation of resources/time
- Responding to private litigation/ potential class actions
- Responding to federal and state regulatory bodies

Four Types Of Threats

- Data Breaches (unauthorized disclosure of personal information)
- Security Incidents (malicious attacks directed at a company)
- Privacy Violations (alleged violation of consumer privacy)
- Phishing/Skimming incidents (individual financial crimes).

STATISTICALLY, of all cyber incidents data breaches are by far the most common, dwarfing rates of all other cyber events.

Who Does This Stuff to Us?

- Next attacker—someone you thought you could trust
- Competitors
- Outside criminal element/ foreign and domestic/ bored teenager
- State Sponsored Activity
- HUMAN ERROR

Mixed motives—financial gain, inflicting physical damage, stealing intellectual property, spreading political protest

Dealing With Threats

- There is no 100%
  - Compliance ≠ Security
- Prioritize business objectives w/in risk tolerance
- Management of contractual relationships/terms
- Proactive Security Plan with technology and policy
  - Coordinated and tested incident response plan
- Prepare Response to the Inevitable Attack
  - Understand threat landscape
  - Access right resources and skills
- Promote Culture of Security Awareness
  - Train
  - Avoid careless mistakes
  - Protect key IP and business assets

Legal Management Issues

- Effective Privacy Notices
- Industry Specific Regulations
  - Federal
  - State
- Assessment of Legal Duties/ Disclosure
- Determination of Key Areas for Cyberinsurance
- Contractual Matters
  - Indemnification
  - Limitation of Liability
  - Risk Transfer
  - Representations & Warranties
- Acquisitions- Due Diligence

Legal Ramifications

- PRIVATE LITIGATION
  - Suppliers, commercial customers
  - Consumers, individuals, class actions
- GOVERNMENT INVESTIGATIONS
  - State laws/ Attorney General Actions
  - Federal Laws/ FTC and Industry Specific Regulations
  - Privacy Actions
  - Criminal Violations

In federal courts approximately 1700 pending legal actions over 50% are private civil actions, 17% are criminal actions.

Real Life Lessons From The FTC

- LABMD, A clinical laboratory, experienced unusual data breaches that compromised personal, medical information of 9300 consumers. The FTC's decision, relying on extensive expert testimony, found that from 2005 to 2010 LabMD failed to:
  - maintain file integrity monitoring;
  - provide intrusion detection;
  - monitor digital traffic across its firewalls;
  - delete no longer needed consumer data;
  - provide security training to employees;
  - implement a strong password policy (a number of employees used the same password "labmd");
  - update its software to deal with known vulnerabilities;
  - control administrative rights to employee laptops and allowed employees to download any software, business related or not;
  - prevent use of peer-to-peer software (LimeWire), which enabled download of a file containing 1,718 pages of confidential information on approximately 9,300 consumers

Lessons From LABMD

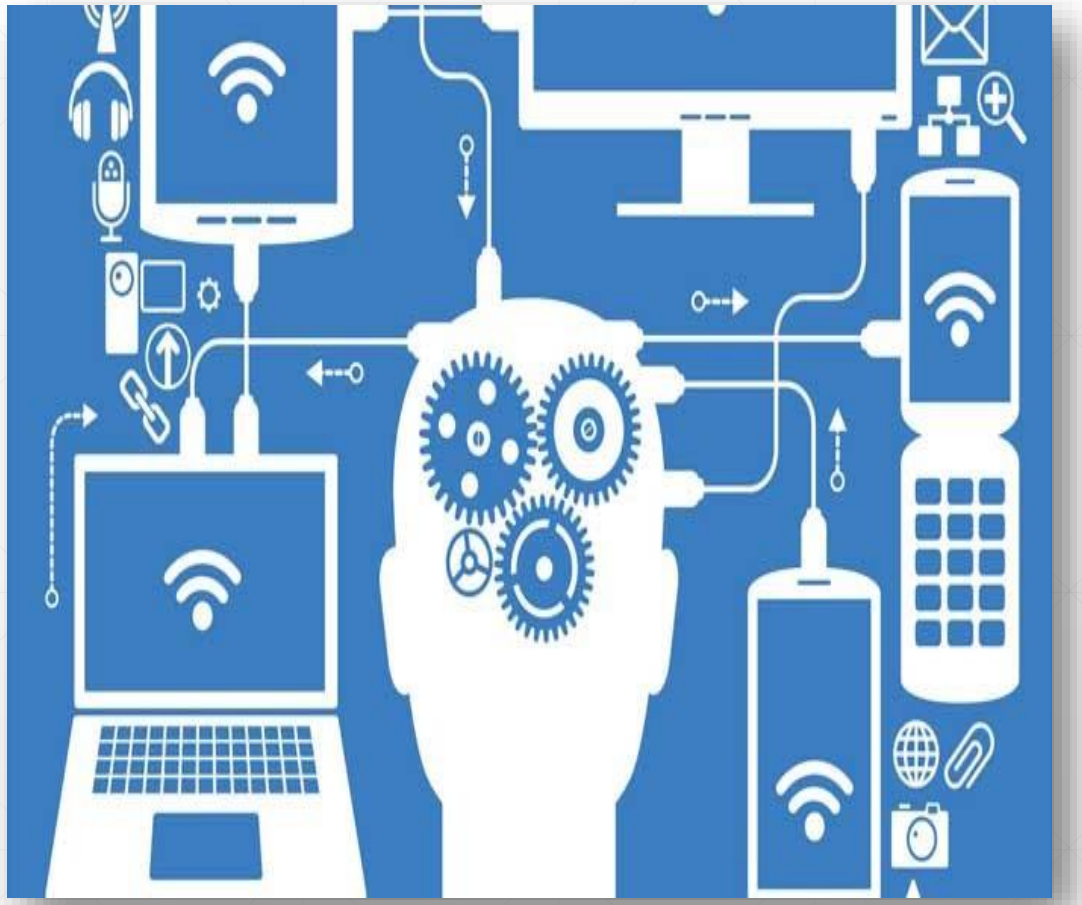
- FTC has made it clear that any industry in possession of sensitive consumer data (such as names, addresses, dates of birth, Social Security numbers, and insurance information) will be required to maintain reasonable data security practices
  - Enforcement actions may result even if there has been no identifiable harm to the subjects of such data.
  - the FTC is going to assert its authority expansively and stay in the cyber cop business.
  - In a data breach case, no actual harm is necessary.
  - Employers must train their employees on infoSEC
  - COMPANIES MUST establish reasonable protocols commensurate with their risk profile to try to protect against cyber intrusions.

Role Of Management And Board

- Duty To Maintain, Grow, And Protect The Assets Of The Company
- Public Company Risks
  - Failure To Maintain Adequate Controls
  - Failure To Disclose
  - Failure To Investigate And Make Informed Judgments
- Shareholder Actions And Derivative Claims
- Government Focus On Individual Liability
- Indemnification Issues

What You Need in Place in Before, During & After

- Management commitment
  - Clear lines of communication
  - Set infosec as an organizational priority
- Specialized knowledge
  - Business compliance and continuity plans
  - Policies and procedures for data protection
  - Statutory compliance by industry/profession/location
  - Employee training/ response teams
- WHEN THE INFORMATION SECURITY/CYBER PROBLEM HAPPENS (and it will)
  - 24/7 responsiveness w/ resources
  - Ability to contain harm/ calm management of crisis
  - Guidance on legal duties/notification/reputation management
  - Dealing with government bodies
  - Positioning/shaping facts w/future litigation in mind
- Avoid exorbitant costs/ potential liabilities



HEPLERBROOM LLC
PROVEN LAWYERS IN THE RIGHT PLACES

THINK IN THREE PHASES

HEPLERBROOM LLC
PROVEN LAWYERS IN THE RIGHT PLACES

Questions / Contact Information:

Glenn E. Davis
Lead Partner
HBCyberGroup
www.HeplerBroom.com |
glenn.davis@helperbroom.com

Direct: 314.480.4154 | Mobile: 314.550.5122

InfoSec Prep: Risk, Reputation, Preparedness

1.01

Why Prepare?

DATOTEL

- Big guys (Target, Schnucks) have been hacked
- My company is small
- I do not have to worry

You are wrong!!

IT Infrastructure

- Includes all components
- Not just limited to desktops or laptops
- Includes mobile devices as well
- Servers, on-site, off site or in the cloud
- E-mail records, files attached to said messages
- Internal IT infrastructure, servers, routers, copiers

How To Prepare-Pre Event

DATOTEL

- Define current environment
- Decide what type(s) of attack to prepare for
- Conduct what-if scenarios
- Decide what risk factors are for each scenario
- Attack shortcomings on a priority basis
- Test systems to make sure systems work as designed
- Update on a regular basis
- Make sure the environment has an “owner”

Define Current Environment

- Firewall configuration
- Anti virus in-place, business grade
- Software security updates installed
- Backups in-place and functional
- Disaster recovery plan in-place and verified
- Redundant systems, connectivity
- Redundant systems, storage
- Servers contain PHI? Are they encrypted/monitored?
- Includes desktops, laptops, mobile devices

What Attacks To Consider

DATOTEL

- Business dependent
- Internal employee attacks
- Phishing attacks
- Crypto Locker
- Unpatched software
- DDoS
- Malware
- Botnets
- Hacktivists, and the list goes on…

Conducting What If Scenarios

DATOTEL

- Technical team needs to do this
- Hire ethical hackers
- Look at system architecture for responses
- Learn from other breaches
- Learn from industry groups
- Penetration testing at some frequency
- Test restored backup files
- Conduct disaster recovery simulations

Scenario Risk Factors

- What is the probability of a specific attack?
- What data, information, IP would be lost?
- What is the cost to recreate the lost information?
- Small and medium sized companies DO get hacked!
- Are there employees, current of former with agendas?
- How aware are employees of the risks?
- What company functions are the most critical?

Setting Organizational Priority

- Importance of potential breach area; H M, or L
- Probability of potential breach; H, M, or L
- Allowable time delay for recovery; Short, Medium, Longer
- Number of people impacted; H, M, or L
- Number of company functions impacted; H, M, or L
- Ability of company to generate revenue; H, M, or L
- Safety (all types) of the client; Critical, Medium, or Low
- Build matrix of all factors, rate 1-5, 5 being high or critical
- Address those items with the highest number first
- Implement fixes accordingly

Test Fixes for Verification

DATOTEL

- Verify the fix has been fully implemented
- Design test scenario
- Testing party should NOT be that who did the fix!
- Verify desired result
- If successful retest at some frequency
- If unsuccessful, address failure, repair, retest

Follow up Is Critical

- Set some schedule for retesting based on criticality
- Make sure this process has an owner
- Make sure the owner has authority and support
- Include this as part of the strategic plan
- Address as part of internal SWOT analysis
- Be sure to consider legal, insurance, and messaging issues as these items are addressed

Questions / Contact Information:

Don Guenther
Datotel
Colocation | Cloud | Service Desk | Managed Services
www.Datotel.com | dguenther@datotel.com

Direct: 314.802.1700 | Mobile: 314.369.9181

Cyber Insurance: Increasingly Relevant in 2016— Why should executives consider coverage?

Lockton Companies

What Can Cyber Insurance Cover?

Insurable assets:

- Personally identifiable information and/or protected health information of employees or consumers
- Corporate Confidential Information

Data breach response costs to include the following:

- Notification mailings & call center
- Credit monitoring
- Credit Correction
- IT forensics
- Public relations
- Defense costs and civil fines from a privacy regulatory action
- Defense costs and damages from civil litigation

What Can Cyber Insurance Cover?

Corporate information technology network:

Addresses the loss of income as a consequence of network downtime. Certain insurers will also extend coverage to downtime of vendors on whom a policyholder is reliant. This is commonly known as “contingent business interruption.”

- Costs to restore compromised data
- Reimbursement for costs associated with an extortion threat

Operational technology:

A few insurers have begun to extend coverage beyond the information technology network to also include operational technology such as industrial control systems.

What Can Cyber Insurance Cover?

Reputation and Brand:

Insuring reputational risk from some form of cyber event remains out of the scope of the majority of insurers. At the time of writing, the London market has begun to innovate to address the financial loss after adverse media publicity. However, capacity remains constrained at $100,000,000 at best.

Physical Assets:

Cyber security is no longer just about risks to information assets. A cyber attack can now cause property damage that also could lead to financial loss from business interruption, as well as liability from bodily injury or pollution, for example.

An assumption that coverage should rest within a property or terrorism policy may not be accurate. Exclusionary language has begun to emerge and is expected to accelerate across the marketplace as losses occur. Dedicated products also have started to appear.

Insuring Agreements Available in Insurance

Network Security Liability
- Claim expenses and damages arising from network and non-network security breaches

Multimedia Liability
- Claim expenses and damages arising from personal injury torts and intellectual property infringement (except patent infringement)
- Claim expenses and damages arising from electronic publishing (website) and other dissemination of matter

Privacy Liability
- Claim expenses and damages emanating from a violation of a privacy law or regulation
- Common law invasion of privacy or infringement of privacy rights

Privacy Regulatory Proceedings + Fines
- Claim expenses in connection with a regulatory inquiry, investigation or proceeding
- Privacy regulation civil fines and consumer redress fund
- PCI DSS fines and assessments

Technology E&O/Miscellaneous E&O
- Claim expenses and damages emanating from a wrongful act in the performance of or failure to perform technology services or other professional services.
- Claim expenses and damages emanating from your technology products' failure to perform or serve the purpose intended

Data Breach Expense Reimbursement
- Expense reimbursement for third-party reasonable and necessary costs including:
- Public relations costs
- Legal and forensics expenses
- Credit protection, mailing and tracking, call center, etc.
- Address three scenarios—mandatory, contractual and voluntary

Cyber Extortion
- Reasonable and necessary expenses and any funds paid in connection with an extortion attempt

Network Business Interruption + Data Restoration and Reputation Harm
- Loss of net income and Extra Expense

What Does Cyber Insurance Not Cover?

Intellectual property assets

Theft of one's own corporate intellectual property (IP) still remains uninsurable today as insurers struggle to understand its intrinsic loss value once compromised.

Cyber Attack Exclusion Clause

Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive.

Questions / Contact Information:

Brad Kosem
Lockton Companies
Insurance | Risk Management | Employee Benefits
www.Lockton.com | bkosem@lockton.com

Direct: 314.812.3818 | Mobile: 314.412.7878

The Risk of Risks:
Reputation Risk Resiliency

Managing the message!

A strong reputation enables your business to meet its goals

- The intangibles can comprise more than 60% of a company's value
- Public perception impacts profitability, book value, sales
- Strong reputation can result in strong stock price growth
- Investors use reputation in purchase decisions
- A strong reputation can be a competitive differentiator

Reputation is owned by stakeholders

- **Reputation = judgments and perceptions of others**

- Customers
- Suppliers
- Investors
- JV partners
- Agents
- Distributors
- Advocacy groups
- Regulators
- Policymakers
- General public

Organizational challenge to managing reputation risk

Reputation literacy not on the risk agenda

Risk literacy not on the reputation agenda

A resilient organization manages all types of risk

Operational Resiliency	Reputation Resiliency
Ability to manage risks and function/adapt throughout the lifecycle of operational disruptions	Ability to maintain good stakeholder perceptions and supportive behavior at all times

Blind spots about reputation risk and data breaches

- Thinking you can wait until an event unfolds to determine how to handle it.
- It’s only a worry for the IT department.
- Everyone knows data breaches happen and that they aren’t our fault.
- We give a lot of money to the community. They know we’re a good company.
- Our budget is focused on hardening our network. We don’t need to invest in crisis planning.

Protecting reputation against risk makes good business sense

“Overall, costs associated with

remediating a reputational event

can be two to seven times higher

than costs related to the operational failure

that caused the reputation damage in the first place.”

The cost of remediation of reputation risk far exceeds the cost of the initial failure.

RIMS 2016 (Risk & Insurance)

True cost of a healthcare breach: $700/compromised record *(Ponemon Institute 2016)*

- Clinical: fraudulent claims processed; inaccurate diagnosis; bad data in research
- Operational: Cost of new hires; cost of training; cost of reorganization
- Legal/regulatory: OCR fines; state fines; loss of accreditation; cost of lawsuit
- Financial: Remediation; communication; insurance impact; changing vendors; business distraction
- Reputational: Loss of patients (average 7%); loss of current/new customers; loss of partners; loss of staff; negative press; see all other costs above.

How to protect your reputation for the inevitable data breach

- A data breach will happen; if you plan ahead you will react more quickly and it will cost you less.
- Invest in a strong cybersecurity program now to protect your reputation later. You don’t want to be the organization that says publicly, “We didn’t know.”
- A strong reputation for preparedness may result in better relationships with regulators.
- Reputation is about how you make decisions when no one is looking. It’s not just about PR, philanthropy or advertising.
- Reputation resiliency happens when you invest as much effort in managing it before, during and after events, just like you do for other key assets.

The key to protecting reputation

Build Enterprise-Wide Reputation Competence.

Prepare before a reputation risk event so you can manage during and after the event: Key steps

Questions/Contact Information:

Beth Rusert
Standing Partnership
Building, protecting and restoring reputations
www.StandingPartnership.com
Brusert@StandingPartnership.com

DATOTEL

710 N. Tucker
Suite 400
St. Louis, MO 63101

314.241.9101 Phone
314.421.7111 Fax
www.datotel.com

Breach Education Alliance speaker background and biographies, R6, 1016

We may be accustomed to hearing about cyber attacks on large firms such as Target, Yahoo and even the federal government. However, data breaches and attacks are not just about the large organizations. Any business of any size can be at risk, but it can be daunting to know the most important steps to take. The Breach Education Alliance can help.

Cyber criminals are everywhere. Business owners can either do nothing and hope for the best, or prepare their organizations properly. The Breach Education Alliance is a group of experts in legal protection and compliance, forensic information security, insurance, reputation management and messaging, and IT infrastructure. They provide practical guidance on steps organizations should take to avoid, minimize, or respond to cyber threats and information security vulnerabilities. These subject matter experts share their expertise as speakers to trade groups, business associations and others who feel unprepared to respond to cyber attacks.

They help you answer the following questions:

- What are your legal requirements duties to protect sensitive business or personal information?
- How do you protect yourself in agreements with vendors and others? What type of government enforcement should you know about?
- What should you insist be included in your insurance policy? Are you familiar with exclusions and liability limits that exclude payments involving data breaches or other cyber intrusions? What precautions do you need to take to support coverage?
- Do you have proper backup files and a plan for disaster recovery? Is your firewall in-place and updated with the latest threat prevention updates?
- When an attack occurs what will you say to your stakeholders, the public and clients? How much will an attack damage your reputation?

The Breach Education Alliance:

Reputation Management: For 25 years Standing Partnership has helped organizations protect their reputations. With deep experience in crisis communications strategy, planning and management as well as digital marketing and communications strategies, Standing clients are typically in environments marked by change that has resulted in the market not seeing them in the way they'd like to be seen. This gap costs them in terms of regulation, litigation and reputation.

IT Infrastructure: Datotel is a managed service company in St Louis providing small to medium sized businesses with IT support, security products and management of critical IT functions.

Legal Protection: HeplerBroom LLC, traces its history to 1894 and has 150 attorneys in its offices located in Missouri and Illinois. The HBCyberGroup, applies its experience and knowledge to a wide range of cybersecurity, data breach and privacy protection legal issues, scaled to specific client needs, including: insurance coverage, legal duties under applicable

federal and state cyber laws and regulations, compliance with industry protocols, emergency response strategies and communications, class action and other litigation defense, privacy protection, identity theft response, trade secret protection, computer fraud and tampering, contracting and payment practices, employment issues, product liability and the Internet of Things, contractor and vendor policies, company Information Security Policies, Response Plans & Procedures, and social media.

Forensic Information Security:

Parameter Security™ is an award-winning ethical hacking firm born out of the need to better protect our businesses, government, health care, financial and educational institutions as well as various organizations globally from vicious hackers. As Professional Ethical Hackers, we emulate the minds and motives of malicious attackers to test the security of your network and employees. We are a 3rd Party Independent services provider, agnostic to hardware, software and tools. Parameter is everything "hacking and security", providing network/web application assessments, regulatory compliance assessments (PCI DSS, HIPAA, GLBA and SEC, FISMA, CJIS, etc.), forensic investigation and breach response.

Cyber Insurance:

Celebrating their 50th Year, Lockton, headquartered in Kansas City, Missouri, is the world's largest privately owned insurance brokerage firm. Lockton's success flows from its commitment "to provide the most uncommon results and service in the most common business". With some of the leading specialists in insurance, risk management, employee benefit consulting and retirement services, Lockton is dedicated to providing the highest level of expertise and service in increasingly complex industries. Lockton's teams take a holistic approach to understanding your unique business exposures, and partners with clients to develop risk transfer strategies that align with corporate directives and initiatives. Lockton's Global Cyber Practice developed one of the first broker proprietary cyber insurance policy forms underwritten by Lloyds of London and was a key stakeholder in the creation of the U.S.' first federal cybersecurity framework.

DATOTEL

710 N. Tucker
Suite 400
St. Louis, MO 63101

314.241.9101 Phone
314.421.7111 Fax
www.datotel.com