
WEBINAR
CYBER & PRIVACY LIABILITY INSURANCE WEBINAR
COMPLIANCY GROUP 3.11.14
PRIVACY PROFESSIONALS LLC

Our Services

- Risk Assessments
- Employee Training
- Automated Incident Response Planning
- Cyber & Privacy Risk (CPR™) Insurance Services

PRIVACY PROFESSIONALS LLC

The Threat Landscape

- “Our nation is at risk. Our infrastructure is at risk. And we as a nation, I think, have not adequately responded to it. It is only going to get worse. The danger is only going to be heightened.” – US Attorney General, Eric Holder
- "High-profile targeted attacks on enterprises are becoming increasingly widespread. Thousands of businesses have already been hacked and had their sensitive data stolen – resulting in multi-billion dollar losses.“ – Eugene Kaspersky, CEO, Kaspersky Labs
- “2014 promises to be a prolific year for cybercrime with mobile threats looming large.” – Trend Micro
- “And from pubs to public agencies, mom-and-pops to multi-nationals, nobody was immune.” – 2013 Data Breach Investigations Report

The Business Impact

- Just one false click is all it takes for an organization to fall victim to today's advanced attacks. Even organizations that follow best practices and deploy the tightest security protocols have been breached.

- A data breach is a traumatic event that can paralyze the entire enterprise, damage relationships with vendors and partners and severely diminish consumer trust. Costs and financial losses associated with data breaches, depending on the size of the organization, can be significant and may take years to recover from. The enterprise trauma can be compounded by lack of a strategic incident response plan.

- Businesses must be able to rapidly determine the nature and scope of a data breach, take immediate steps to contain it, ensure that forensic evidence is not accidentally ruined, notify regulators, law enforcement officials and affected individuals, and the impacted users of the compromised data.

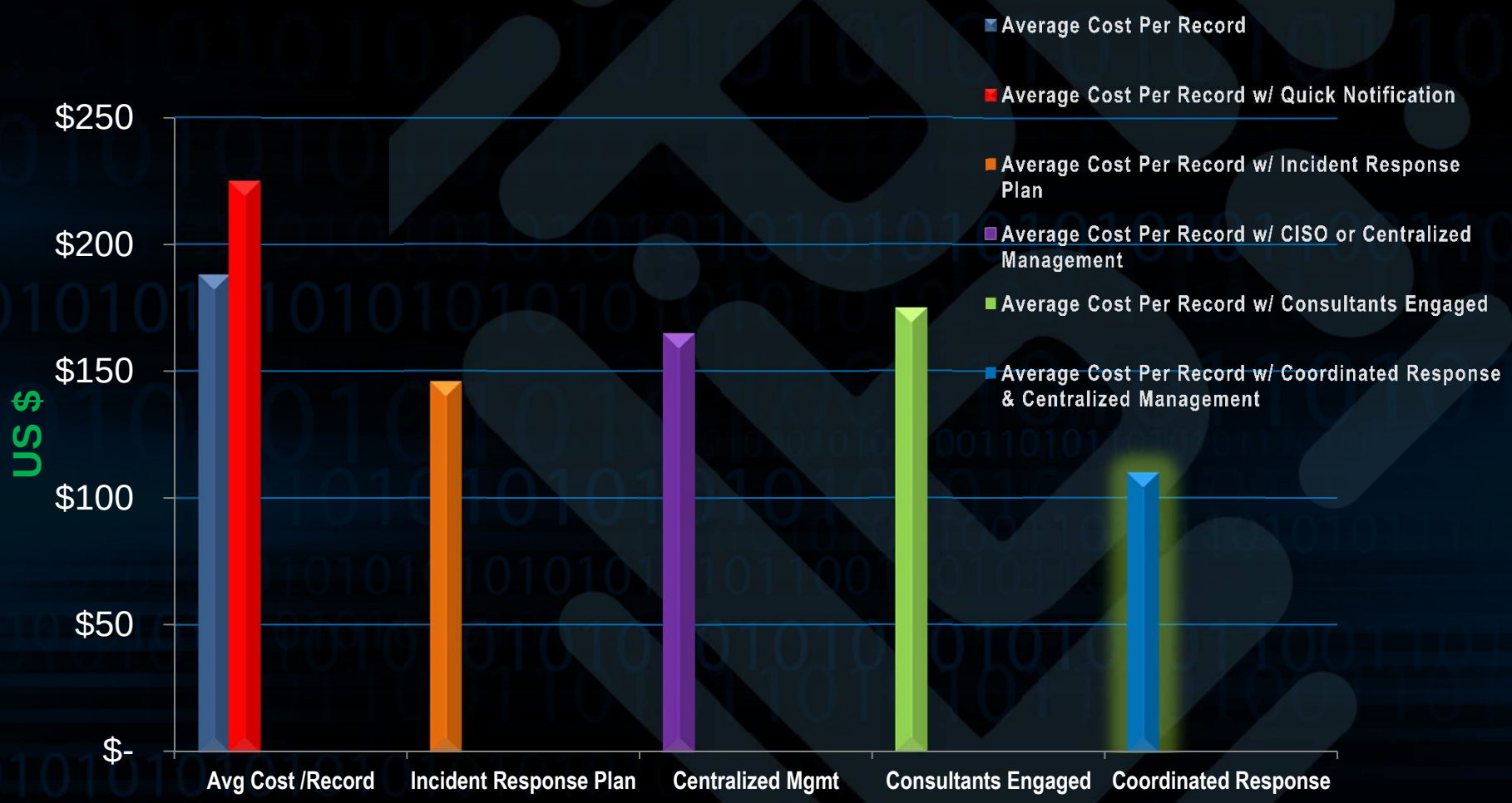
WHY INSURE?

PRIVACY PROFESSIONALS LLC

Data privacy and security breaches impact the entire enterprise – shareholders, employees, customers and the bottom line!

PRIVACY PROFESSIONALS LLC

The Financial & Reputational Impact

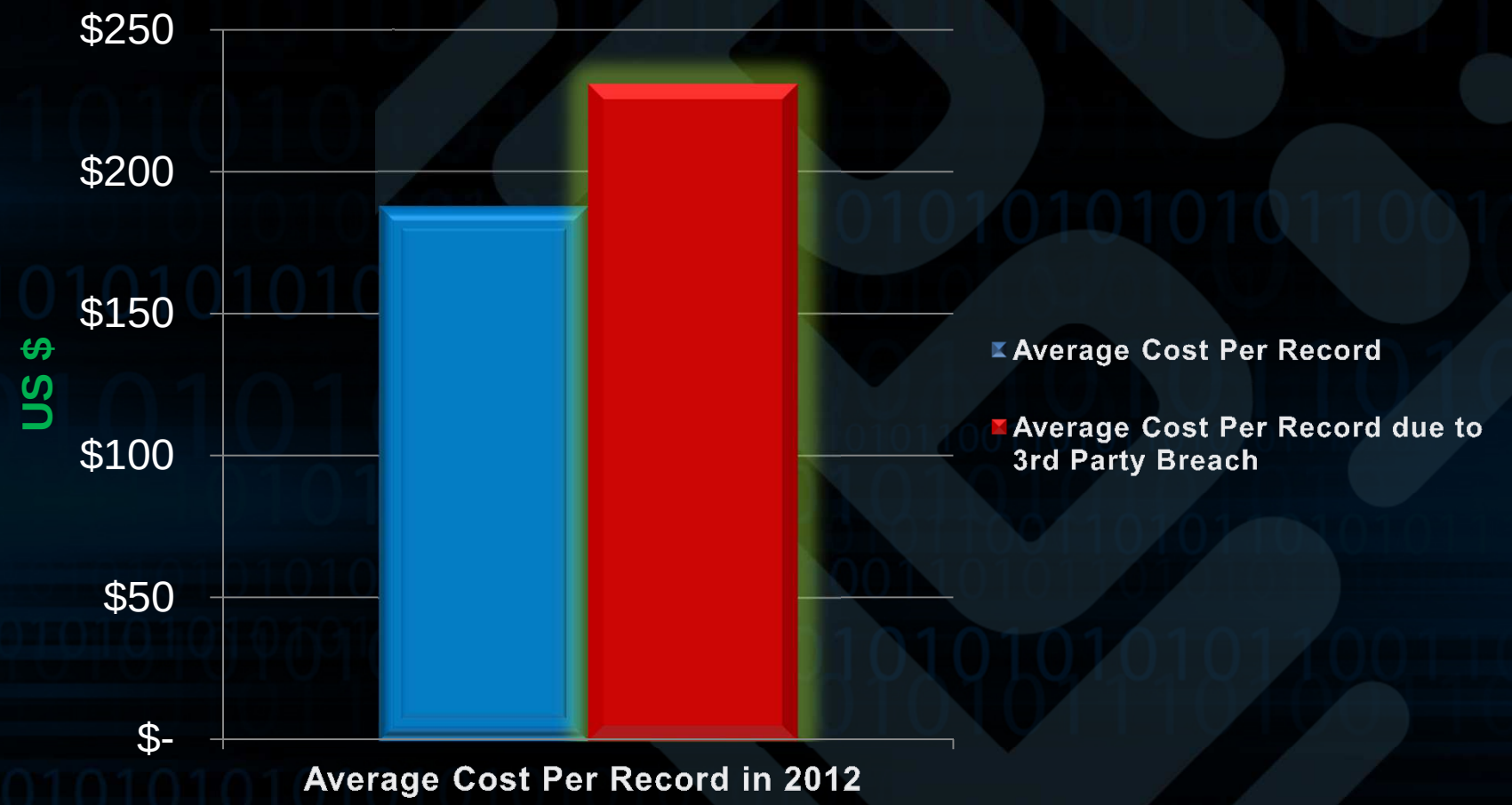


PRIVACY PROFESSIONALS LLC

The Third Party Risk

- Our information economy exists in a complicated matrix of information transfers and relationships. Outsourcing of critical infrastructure, processes and operations to third-party service providers is now a common business practice. Outsourced functions may include:
  - Credit and Debit Card Payment Processing
  - Cloud Technologies
  - Managed Information Technology/Security (SaaS)
  - Accounting
  - Human Resources
  - Healthcare Industry: Claims Administration, Billing, Collections, Wellness Programs, etc.

The Third Party Risk



PRIVACY PROFESSIONALS LLC

The Third Party Risk

- What happens if there is a breach of customer/patient/client non-public Personally Identifiable Information (PII) or Protected Health Information (PHI) at the vendor level?

  Typical Responses:
  - We have a contracts with all our vendors and they are responsible.
  - We are a Covered Entity under HIPAA and our Business Associate Agreements with our vendors protects us from data breaches.

- Regulatory compliance and many legal liabilities cannot be contractually transferred to third-parties. While a solid contract requiring a vendor to indemnify the data owner for breach responses costs is good risk management – data owners are ultimately legally required to comply with all regulatory notification and breach response obligations.

The Small and Mid-Sized Enterprise Risk

- Target, Adobe, Google, Facebook, Yahoo, Sony, TJ Maxx, Citibank, Global Payments are well known brands that suffered well publicized breaches. The national attention to these breaches created the notion that Cyber & Privacy risk is only a real concern for large or publicly traded organizations. While the big guys may steal the headlines, it's the small to mid-sized organizations that should be most concerned because they are least prepared.

  2012: 72% of breaches occurred at companies with less than 100 employees.
  2013: 52% or breaches occurred at companies with less than 1,000 employees.

PRIVACY PROFESSIONALS LLC

The Small and Mid-Sized Enterprise Risk

- Regulators are targeting organizations of all types and sizes
  - In 2013, the Office of Civil Rights (OCR) issued a $150,000 fine against a small clinic, Adult & Pediatric Dermatology, for a breach of just 2,200 health records.
  - LabMD forced out of business due to an FTC investigation involving just 9,000 health records.
  - In 2013, Hospice of North Idaho, agreed to pay a $50,000 penalty following a theft of a laptop that exposed only 441 PHI records, which was the first federal investigation involving a PHI data breach that affected fewer than 500 individuals.

The Need for Cyber & Privacy Risk Insurance

- The alarming growth in cybercrime and data breaches highlights the challenges that all business leaders face. Small and large organizations alike are at risk and not being prepared can have grave financial consequences.
- Its all about preparation:
  - A properly designed Cyber & Privacy Risk Insurance Program

    +
  - Having an integrated incident response plan in place before data is compromised

    =
  - Significantly mitigates financial losses and minimizes reputational damage.

PRIVACY PROFESSIONALS LLC

Cyber & Privacy Liability Insurance Market Overview

- The Cyber & Privacy Liability insurance market has evolved over the past decade, but it is still a relatively new market. The current marketplace includes various products that range from stand-alone Cyber Liability policy forms to products that can incorporate other third party liability coverage parts, such as Technology Errors & Omissions, Medical Malpractice, Managed Care Liability, Professional Liability, Media Liability and Management Liability forms.

- The marketplace continues to expand in an effort to keep pace with advancing privacy and data security threats, cybercrime and the ever changing regulatory environment.

Cyber & Privacy Insurance Program Elements

- **First Party Coverage Parts**
  - Data Breach Loss Mitigation Fund
  - Business Interruption
  - Digital Asset Loss
  - Cyber Extortion
  - Regulatory Fines & Penalties

- **Third Party Coverage Parts**
  - Network Security Liability
  - Privacy Liability
  - Media Liability
  - Legal Defense for Regulatory Actions

Cyber & Privacy Insurance: First Party Insuring Agreements

- **Data Breach Loss Mitigation Fund**

  - ✓ Legal Consultation - Data Breach Coach
  - ✓ Forensic Investigation Services
  - ✓ Communication to Affected Individuals – Notification
  - ✓ Credit Monitoring
  - ✓ Identity Theft Restoration Services
  - ✓ Call Center Services
  - ✓ Public Relations Services
  - ✓ Crisis Management Services

Cyber & Privacy Insurance: First Party Insuring Agreements

- **Business Interruption**

  Indemnification for loss of income and incurred extra expenses that arise directly out of a network security breach.

- **Digital Asset Loss**

  Indemnification for costs to recreate, rebuild or recollect digital information assets.

- **Cyber Extortion**

  Covers extortion monies and associated expenses arising out of a criminal threat to release sensitive information or bring down a network unless such consideration is paid.

- **Regulatory Fines or Penalties**

  Indemnification for fines and penalties imposed by federal or state agencies for non-compliance with privacy regulations. (PCI fines are not automatically included.)

Cyber & Privacy Insurance: Third Party Insuring Agreements

➢ Network Security Liability

Affords defense and indemnity coverage for third-party claims alleging failure to protect against transmission of malicious code, denial of service attacks and unauthorized access and/or use of computer systems.

➢ Privacy Liability

Affords defense and indemnity coverage for third-party claims alleging negligent handling of non-public Personally Identifiable Information (PII) including:

- ❖ Protected Health Information (PHI)
- ❖ Confidential Employee Information
- ❖ Third-Party Corporate Confidential Information

➢ Regulatory Defense

Affords legal defense for post breach regulatory actions brought by federal regulators such as HIPAA/HITECH, COPPA, FTC or state attorney generals (SAG).

Traditional Insurance Implications: Professional Liability

➢ Professional Liability

Affords coverage for claims made by third-parties alleging financial loss arising out of the policyholders performance or failure to perform professional services. Cyber & Privacy Liability claims may be covered if a data breach arises out of the policyholders performance of professional services and not otherwise excluded.

➢ Common Professional Liability Policy Forms

- ❖ Specified Professions Liability: Medical Malpractice, Lawyer Professional, Accountants Professional, Healthcare Professional
- ❖ Miscellaneous Professional Liability (Unspecified Professions): Real Estate Errors & Omissions, Management Consultant, Caterer, etc.
- ❖ Technology Errors & Omissions Liability: Technology Service Providers, these policies can include broad CPR coverage.
- ❖ Media Liability: Publishers, Broadcasters, Bloggers, these policies can include broad CPR Coverage.

Traditional Insurance Implications: Crime/Fidelity

➢ Crime/Fidelity Bonds

- ❖ Crime or Fidelity policies are designed to provide coverage for employee theft of money, securities or other property including forgery, robbery, computer fraud, wire transfer fraud, embezzlement, etc.
- ❖ While a material percentage of breaches involve fraudulent actions of employees (theft of data, left of laptops or other devices) that may trigger some form of coverage, these do not cover loss of data.
- ❖ A majority of crime policy forms now contain specific data breach exclusions.

Traditional Insurance Implications: Management Liability

➢ Management/Executive Liability/Directors & Officers Liability

- ❖ A number of insurance carriers are now offering Cyber & Privacy Liability coverage as part of a "package" of Executive Liability coverages including:
  - ✓ Directors & Officers Liability
  - ✓ Employment Practices Liability
  - ✓ Fiduciary Liability
  - ✓ Professional Liability
  - ✓ Crime
  - ✓ ERISA Fidelity
  - ✓ Kidnap & Ransom
- ❖ This may be a cost effective solution, but buyers should weigh their options carefully and consider the risks of the "all eggs in one basket approach", as aggregate limits of liability may apply to all coverage parts.

Traditional Insurance Implications: Property & Casualty

- A Commercial Package Policy (CPP) can include many coverage parts. Typically, a CPP policy under the Property Coverage Part affords coverage for direct physical loss or damage to covered property; and the General Liability Coverage Part responds to claims alleging legal liability for Bodily Injury, Property Damage, and Advertising Injury & Personal Injury.

- Under the CPP policy form, Electronic Data is not considered tangible property. Since 2004, CPP policies contain an Electronic Data Exclusion, which eliminates coverage for claims arising out of loss, damage to, or the inability to access electronic data.

- The Advertising & Personal Injury Insuring Agreement under a CPP policy may afford limited coverage for liability claims, but only under certain conditions. For example, coverage may apply if a data breach involved a "publication" and violated an individuals "right to privacy", which resulted in emotional distress (bodily injury) or personal injury (libel, slander, defamation of character), but no coverage would apply if the claim centered on the theft of data.

Traditional Insurance Implications: Wake Up Call

- Recent lawsuits filed by General Liability carriers against their policyholders that suffered data breaches should serve as a wake up call:
  - Zurich filed suit for injunction against Sony in the wake of their breach
  - Liberty filed suit for injunction against Schnucks in the wake of their data breach.

Questions?

PRIVACY PROFESSIONALS LLC

Gamelah Palagonia, CIPM, CIPP/IT, CIPP/G, ARM, RPLU+, Founder
(646) 354-7065/gpalagonia@privacyprofessionals.com

Zach Scheublein, CIPP/US, Vice President
(646) 354-7066/zscheublein@privacyprofessionals.com

www.privacyprofessionals.com

Source Information - Slides 8 & 10: Ponemon Institute (1) 2013 Cost of a Data Breach Study Global Analysis (2) The Human Factor in Data Protection

PRIVACY PROFESSIONALS LLC