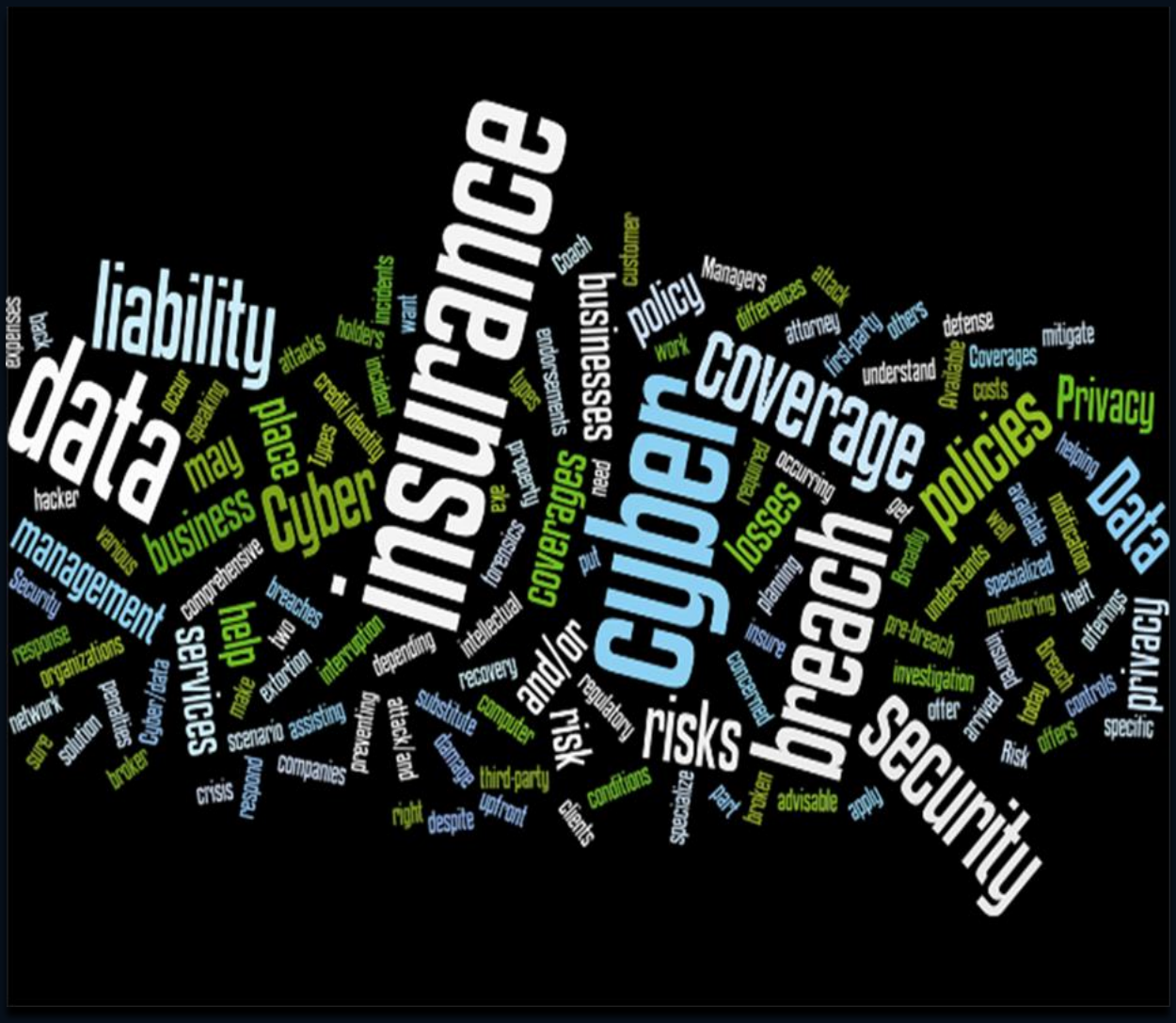
2014

Cyber Data Risk Managers 2014

Data Privacy, Information Security and Cyber Insurance Trends Report

(3rd Annual Edition)



Cyber Data-Risk Managers LLC

Contents

Executive Summary

Cyber Data Risk Managers is a specialist U.S. insurance broker focused exclusively on cyber/data breach and intellectual property insurance that seeks to connect businesses and public and private organizations of all sizes, industries and sectors, as well as industry experts in the area of Data Privacy and Information Security with effective insurance solutions to help mitigate cyber risk, data breach and intellectual property risks.

Today, more than ever businesses and organizations need to stay one step ahead of online attackers and other malicious actors. There's ample evidence all around us that proves adversaries are coming up with new and much more sophisticated methods for distributing malware, while remaining undetected for long periods and stealing sensitive customer data, intellectual property or disrupting critical systems.

This 3rd annual Cyber Data Risk Managers 2014 report, released on Data Privacy Day January 28, 2014 shows our commitment to data privacy and our continued support to help empower businesses and organizations to make the protection of privacy and data a great priority in their environments. Included in this report, are many invaluable insights and recommendations offered by Data Privacy and Information Security industry experts that will prove useful for businesses and organizations, regardless of industry or sector.

Insights and recommendations discussed include:

- **Buying Cyber Insurance and Intellectual Property Protection in Today's Rapidly Evolving Threat Environment**
  by Christine Marciano, President/CEO, Cyber Data Risk Managers
- **Understanding the 2014 Threats, Risks and Importance of Incident Response** by JD Sherry, Vice President, Technology & Solutions, Trend Micro
- **The Often Forgotten About Data Breach Weak Spot: Disposal of IT Equipment** by Judy Selby, Partner, Baker Hotelster
- **Inadequate Protection of Sensitive Data has Increasingly Expensive Consequences, Several Tips to Consider**
  by Barry Schrager, President, XBridge Systems

Executive Summary

(continued)

- **Ad Hoc Incident Response isn't Enough Anymore**
  by Bruce Schneier, Cyber Security Technologist, Author, CTO, Co3 Systems
- **Massive Target Breach Highlights the Importance of Changing to a Chip-Enabled POS System and 2014 is the Year InfoSec Professionals take a Closer Look at All Things Bitcoin**
  by Richard Santalesa, Member, SmartedgeLaw Group
- **Remember that public WiFi networks are not protected. In 2014, make sure you use a VPN for security**
  by Kent Lawson, CEO, Private Wifi
- **2014: The Year New Privacy Risks and Data Breaches Arise Due to Evolving Internet of Things, Big Data, Mobile Apps and Wearable Computing Device Risks** by Rebecca Herold, CEO, The Privacy Professor
- **Data Breaches will continue to dominate the Headlines in 2014 and Organizations must ensure their Security Efforts Measure Up to Specific Control Standards or else Face the Consequences**
  by Anthony M. Freed, Community Engagement Coordinator, TripWire
- **Data Breaches are a Fact of Life in the Digital Age and Organizations will Increasingly be under Pressure by Customers and Governments to become more immune to Cyber Attacks**
  by Michael Fertik, CEO, Reputation.com
- **In 2014, The Voice of the Customer Will Drive Organizations to Reprioritize their Security and Data Privacy Measures or Else Lose their Customer's Business** by Jack Danahy, CEO, Danahy Advisors LLC
- **Simply put, 2014 is the Year to Get Back to Basics and Build a Strong Data Privacy and Security Program**
  by Shaun Dakin, CEO, Dakin Associates and the Privacy Camp
- **Why Understanding a Breach Victim's Mindset is Key to a Successful Data Breach Resolution Plan**
  by Michael Bruemmer, Vice President, Data Breach Resolution, Experian
- **Five Questions for Senior Leadership to Consider on How to bring IT, Physical and Human Security together under a true Information Security Governance Program** by Andy Bochman, CEO, Bochman Advisors
- **Listing of Key Information Security Areas that Must be Assessed at Least Annually** by Ronald Beltz, Vice President, Loricca

Introduction

Buying Cyber Insurance and Intellectual Property Protection in Today's Rapidly Evolving Threat Environment

Cyber attacks, data breaches and patent infringement cases are rapidly increasing with no end in sight and have become the "new normal" cost of operating a business today. If this is not convincing, all one needs to do is check the hourly news reports and will most likely find a newly reported cyber attack, data breach or patent infringement lawsuit. Lately, the question many seem to be asking after recognizing "things happen and are happening more often" is -- "When our cyber attack, data breach or patent infringement lawsuit happens, how will we respond?"

Today, *how* an organization responds to such events is more important than ever. In the pages that follow, many of the other experts have suggested the same. 2014 is the year that organizations need to get an incident response plan in place or else face the consequences for being unprepared. Imagine if you will for a moment, that should a fire occur in your building, there's no doubt you would know who to call and there would be a response team on the way to assist after you made the call. When a cyber attack or data breach happens, it's no different. You need to know who you're going to call, which is why a response team is also needed. A response team will require a forensics investigator, an attorney, a data breach resolutions provider and a PR firm amongst others. Having this team already in place before an incident happens is nonetheless very important today.

Cyber insurance with data breach response services, offers organizations a comprehensive turn-key incident response plan solution. It offers the ability to have all of the response team members on retainer and with just one phone call to your cyber insurance broker to get the response team on its way. Make 2014 the year your organization establishes an incident response plan and buys cyber insurance to help put the response team in place.

Buying Cyber Insurance and Intellectual Property Protection in Today's Rapidly Evolving Threat Environment

(continued)

Traditional Insurance Policies are not meant to cover cyber risks, data breaches or patent infringement lawsuits

There's still somewhat of a misnomer today that a traditional insurance policy covers cyber risk, data breaches and patents. Most traditional insurance policies do not cover cyber attacks, data breaches or patent infringement lawsuits, which is why it is advisable to examine what coverages are held under traditional insurance policies and identify where potential coverage gaps might exist. Why leave it to the court system to determine whether or not your insurance coverage dispute with your insurance company will be granted? Especially when today, the defense costs can be much higher than what it would have cost to purchase a standalone cyber/data breach insurance policy.

Patent Infringements, there's Insurance for that!

Same holds true for patent infringements. Today, obtaining a patent licensing agreement is quickly becoming the "new normal" cost of operating a business today. With today's evolving technology, some may argue that it's hard to determine whether or not you're infringing upon someone's patent. Whether you're a patentee concerned that others may be infringing upon your patent(s) or you're an organization worried you are infringing upon another's patent(s), *there's insurance for that!* With the average cost of determining the validity of a patent in court today hovering around $3,000,000, exploring how patent infringement insurance or other alternative options can help you assert your patent rights or defend an infringement case is highly suggested.

Cyber/Data Breach Insurance is Not One Size Fits All Coverage

Make an educated choice when purchasing cyber/data breach insurance. Just because one policy is cheaper, does not mean it's better. Work with an insurance broker who has expertise and can help you navigate the various policies and coverages that best suit your needs.

Buying Cyber Insurance and Intellectual Property Protection in Today's Rapidly Evolving Threat Environment

(continued)

It's my hope that you find this report not only interesting, but helpful in making 2014 the year in which you establish an incident response plan and take further steps to ensure the protection of privacy and data in your environment. And quite simply, remember, an online attacker usually enters through your network's "back door" or a door you didn't realize you left open *but* the FTC, State Attorneys General and other regulators will no doubt be lining up thereafter knocking on your "front door!" How will you respond?

If you would like to learn more about how I can help you create an incident response plan through the utilization of a cyber/data breach insurance policy or more about the types of patent infringement insurance and/or alternatives that are available, I welcome you to contact me.

Have a safe and secure 2014!

Christine Marciano

President/CEO, Cyber Data Risk Managers

Understanding the 2014 Threats, Risks and Importance of Incident Response

"2014 will see an unprecedented number of major security incidents involving personal and corporate theft. Expect at least one major security breach a month to impact a global audience which is being accelerated through the adoption of cloud and mobility platforms. Much of this is due to innovation and technology outpacing the risk management and security architecture of these ecosystems. Individuals and organizations will demand more of merchants and technology companies in 2014 to help educate as well as collaborate on how we can all stay safe online, maintain the integrity of our identities but still do so in a manner that accelerates productivity and value. Incident response will be key for everyone, regardless if you are a consumer or a large government body protecting national secrets. We will all need to be well-versed on how to handle cyber security incidents to make sure we have protections in place for individual continuity as well as business continuity when these major security incidents impact our lives."

JD Sherry

Vice President, Technology and Solutions

Trend Micro

The Often Forgotten About Data Breach Weak Spot: Disposal of IT Equipment

Policies and procedures for securing IT equipment that stores confidential information have rightly been getting a lot of attention. But one area that deserves more focus is ensuring the security of IT equipment that is designated for disposal. Because data-storing IT equipment has a limited life span before it is remarketed, recycled, or otherwise disposed, entities must develop and implement strong, defensible policies to protect the stored data throughout the entire IT asset disposition process. A solid plan not only reduces the risk of a security incident or data breach, it also provides evidence that adequate safeguards and controls were in place should an incident take place.

Judy Selby

Partner, Baker Hostetler

Inadequate Protection of Sensitive Data has Increasingly Expensive Consequences

Here are several tips to consider in 2014:

1. Make sure you know where ALL copies of your sensitive data reside. Copies have been made for years, and even a year or two old data can be harmful. IBM has estimated that over 70% of data on their mainframe systems is copies.

2. Make sure that all database query and report output, containing sensitive information, is secured properly.

3. Make sure you know everyone who has access to all this sensitive data. Do they really need it to do their job? Minimize access to those with a need to know. Journal accesses from those people, and regularly review the journals.

Barry Schrager

President, XBridge Systems

Ad Hoc Incident Response isn't Enough Anymore. Here's Why –

Incident response is finally coming into its own. There are two trends driving this. First, attacks have gotten more sophisticated, which means response has to be similarly sophisticated. And second, the regulatory environment has gotten more complicated, which means response has to be more regimented and documented. Lastly, one of the real problems with any emergency response system is that it is only used in an emergency, which means that it's real easy to get it wrong. Anything that makes all of this better is going to be real important in 2014.

Bruce Schneier

Cyber Security Technologist, Author

Chief Technology Officer, Co3 Systems

Massive Target Breach Highlights the Importance of Changing to a Chip-Enabled POS System and 2014 is the Year InfoSec Professionals take a Closer Look at All Things Bitcoin

"The massive Target breach was an early 2014 wake up call. With it, the rise of PCI-DSS 3.0 and renewed Congressional efforts on data security legislation, 2014 will see a re-newed focus toward 'smart chip' cards - whether 'chip and signature' or 'chip and pin' schemes - and away from magnetic stripes. Smart companies should start looking into chip-enabled POS systems as soon as possible. And after carefully watching Overstock.com's plan to accept Bitcoin crypto currency this year, the momentum for the currency's wider acceptance will grow - barring a major security incident in connection. As a result, 2014 is the year for InfoSec professionals to dig further into how Bitcoin works and what opportunities it may hold (as well as what perils/security concerns are raised.)"

Richard Santalesa

Member, The SmartedgeLaw Group

Remember that public WiFi networks are not protected. In 2014, make sure you use a VPN for security

Public WiFi hotspot connections are just that -- public. To keep your data safe this Data Privacy Day -- and beyond -- use a personal Virtual Private Network (VPN) to maintain your privacy. A VPN, like PRIVATE WiFi, protects your sensitive information by transmitting it through a secure tunnel which makes it invisible to hackers. That's the only way to safely access a WiFi connection. Download a free 10-day trial now: http://www.privatewifi.com/get-protected/.

Kent Lawson

CEO, Private WiFi

2014: The Year New Privacy Risks and Data Breaches Arise due to Evolving Internet of Things, Big Data, Mobile Apps and Wearable Computing Device Risks

2014 will bring significant new privacy risks and breaches as a result of new gadgets within the Internet of Things, the use of Big Data Analytics on all that data, and the current lack of standards and laws governing how all this new data can be used. It is a goldmine of personal data, and data that can be tied directly to individuals and their daily activities, that marketers and tech companies are drooling over. Each individual needs to become more vigilant about protecting their own privacy. As all these increasingly large recent breaches show, they cannot assume that companies are implementing appropriate controls, and they must realize there is a lack of laws and regulations requiring organizations to protect a large portion of personal data.

Here are some top tips for protecting the data collected about you in the Internet of Things and the use of Big Data analytics on all that data.

For businesses:

- Use the data you collect from individuals... all the data, since data of all kinds may, through the use of Big Data analytics, be tied to specific individuals... *only* for the purposes for which you collected it from them. This is the cornerstone of privacy protection. I know this concept will spark many protests; however, these are the start of some enlightening discussions.
- Put a privacy notice on your website that clearly states what you are going to do with the data you collect from individuals. Avoid those terms that leave the door open to you, like "trusted third parties" or "those who support our business." Be transparent… and then actually do what your notice says you are doing!
- Re-visit your use of so-called "aggregated" or "de-identified" data. Is it really de-identified? How do you know? Are you taking what is truly de-identified data and combining it with other proclaimed de-identified data? If so, you'd better check to see if this new, larger, more data-rich database is still truly de--identified.

2014: The Year New Privacy Risks and Data Breaches Arise due to Evolving Internet of Things, Big Data, Mobile Apps and Wearable Computing Device Risks

(continued)

And some basics that any organization that wants to be trusted and ethical should already be doing:

1. Assign someone, in a position of authority, responsibility for privacy, and who can answer consumer questions and concerns about privacy related to your organization's products and services.
2. Establish strong visible executive support for the privacy program.
3. Post a privacy (not anti-privacy) notice on your website.
4. Establish documented and implemented privacy policies and supporting procedures.
5. Build privacy protections into all the products and services you create to collect data.
6. Provide regular privacy training and ongoing privacy communications.
7. Establish a privacy breach response team, train the team, and test the breach response procedures.

For consumers:

- Check the privacy notices posted on the sites of those who are collecting your data, before you let them collect it whenever possible.
- If they do not have a privacy notice, don't do business with them. Any reputable organization that is collecting data from you should have a privacy notice.
- If all their privacy notice basically does is tell you how they can use your data any way they want, and you do not have any choices, then it really is not a privacy notice, it is a lack-of-privacy notice. Leave them before you lose your data and your privacy.
- Is someone at the organization given responsibility for privacy? If so, that is good; make sure it is more than just an empty title, and that they actually have privacy expertise. If they do not know what FIPPs or OECD are, then they probably have very little in place for privacy protections.

2014: The Year New Privacy Risks and Data Breaches Arise due to Evolving Internet of Things, Big Data, Mobile Apps and Wearable Computing Device Risks

(continued)

- Beware of all those mobile apps! Most of them have few, and usually no, information security or privacy protections built into them. And most will take as much of your personal and associated data from you and then sell it to one to many other third parties, that you don't even know about. Remember, nothing is free… even that cool app. Especially if a mobile app asks you for more data than it reasonably needs to provide you with its service. I've created many different aliases, with bogus personal identities, that I use to download and check out such mobile apps; something you can consider doing as well.
- Never, ever, ever use the same passwords on your mobile apps, social media sites, or gadgets as you use on your work systems, or that you use to get access to bank, financial and other sensitive information.

On a related topic, wearable computing devices also cause me particular concern, especially within healthcare organizations; not only in hospitals and clinics, but within healthcare insurers, and all types of BAs, as well. The quickly growing range of wearables, not only just Google Glass, but also smart watches, and the gadgets used on patients to monitor a vast array of bodily functions and whereabouts, will feed into Big Data analytics to gain insights not only about the health issues of individuals, but could potentially be used inappropriately by others, and could also create attack pathways by those who want to do specific patients harm. Last year Ex-VP Cheney talked about how he made his doctors disable the remote access capability to his pacemaker when he got it a few years earlier because he was afraid hackers would break into it and permanently shut his life off. All organizations need to establish some policies for the use of wearable devices within their work areas, within and outside of their facilities.

Rebecca Herold, CEO, The Privacy Professor
Partner, Compliance Helper
www.PrivacyGuidance.com
twitter

Data Breaches will continue to dominate the Headlines in 2014 and Organizations must ensure their Security Efforts Measure Up to Specific Control Standards or else Face the Consequences

Major data breaches involving millions of compromised records will continue to dominate the headlines, and aside from concerns over diminished brand appeal and revenue losses that occur after such events, organizations should pay greater attention to ensuring they meet and maintain an objective level of due care to mitigate liability, or else face protracted civil actions and punitive regulatory repercussions. The Twenty Critical Controls (formerly administered by SANS, and now the charge of the Council on Cybersecurity) is emerging as the "defacto yardstick by which corporate security programs can be measured," according to the Cybersecurity Law Institute. The 20 CSC provide a broad baseline of technical controls that are required to ensure a robust network security posture, and will prove indispensable for any risk-based security management program. Organizations should make sure their security efforts measure up to this standard at a bare minimum, and further embrace it as the foundation from upon which all other risk management initiatives are based.

Anthony M. Freed

Community Engagement Coordinator, TripWire

Data Breaches are a Fact of Life in the Digital Age and Organizations will Increasingly be under Pressure by Customers and Governments to become more Immune to Cyber Attacks

2013 was eye-opening for people around the world. It was the year of Edward Snowden and the NSA surveillance programs, massive data breaches like Adobe, questions as to how Big Pharma and others are using personal data to target people for drug studies, more scrutiny of Facebook for its privacy policies and use of personal data in ads. If 2013 was the year that woke people up to the question of privacy and personal data, when the wave began to crest, Reputation.com expects 2014 to be when that wave breaks upon the shore. In 2014, there will no doubt be more information on government surveillance - and more pressure on the government for transparency and enhanced oversight. People are coming to understand that data breaches (like Target and Snapchat) are a fact of life in the Digital Age - and that companies and governments hit by attacks are not necessarily negligent. However, there will be increased pressure on large-scale organizations to become more immune to cyber attacks - and to be more communicative with customers about steps they're taking to prevent such attacks, how they use personal data, etc. Likewise, the rise of technologies like Snapchat demonstrates a new and hungry appetite for mechanisms that enable us to participate in digital life while still maintaining a protective layer between us and "the machine." We've just seen word of Silent Circle's Blackphone. The time is ripe for privacy technologists - in terms of customer demand and what is able to be created. It's going to be a very interesting year.

Michael Fertik

CEO, Reputation.com

In 2014, The Voice of the Customer Will Drive Organizations to Reprioritize their Security and Data Privacy Measures or Else Lose their Customer's Business

2014 looks to be the year where the public finally finds its voice in the debate over data privacy and data breach responsibility. The headlines of 2013 were full of events that helped people to draw the line between their private data, their service providers, and the very real fear of exposure and risk. From the Snowden revelations to reports on data mining by Google and Facebook, to congressional testimony about the pervasive vulnerability of the Affordable Care Act website, people were becoming educated. As a result, there is going to be more and more pressure on organizations to ensure the protection of the data that they acquire and develop. We see some of this public pushback already; in Consumer Reports recommending that readers delay entering their information into Heathcare.gov because of security risks, and in Target reporting a loss of consumer sales revenue following their breach report during the holiday season.

The voice of the customer has always been the missing catalyst that companies and organizations needed to drive their reprioritization of their security and data privacy measures. Loose and non-prescriptive regulation has left too much room for interpretation, and penalties were always slow in coming and in many cases meaningless. Real customer backlash, in the form of vocal protest, changes in purchasing behavior, and reticence in sharing information, is the push that well-meaning organizations need to rethink their data acquisition strategies, their investment in protection, and their responsiveness to changes in the threat and vulnerability landscapes. 2014 looks likely to finally be that year.

Jack Danahy

CEO, Danahy Advisors LLC

Simply put, 2014 is the Year to Get Back to Basics and Build a Strong Data Privacy and Security Program

"Get back to basics and make sure that your organization has strong customer privacy and security in place. As we have seen with the Target breach no one can be too complacent! '

Shaun Dakin

Dakin Associates - Digital Strategy

Founder of Privacy Camp

Why Understanding a Breach Victim's Mindset is Key to a Successful Data Breach Resolution Plan

As we have witnessed, 2013 was a year of mega data breaches that will surely bring heighted attention around cybersecurity and subsequent ramifications for businesses in 2014 and beyond. Hopefully the attention and dialogue will contribute to more awareness on how businesses can prepare for a breach and manage the incident response, because unfortunately many companies are still not prepared. According to a 2013 Ponemon Institute study, "Is Your Company Ready for a Big Data Breach?," nearly 40 percent of companies that experienced a breach say they have not developed a formal preparedness plan even - after the incident. There are many considerations to take into account when a breach happens, but one of the most important aspects is to put the affected party at the center of the decision-making. This means putting yourself in the place of your audience and thinking about how they feel and would want to know about the incident. One way to set this mindset into action is to provide a clear and transparent notification letter explaining the breach and what the individual should do to protect themself. Also, consider various remedies such as setting up a call center to handle their concerns and questions. The key in mitigating the fallout is putting your breached audience first. This approach will go a long way in re-building the trust in your organization and protecting your reputation.

"The number of data breaches both experienced and reported is expected to continue to rise, with new security threats and regulations pushing for more transparency on the horizon. All signs are pointing to 2014 being a critical year for companies to better prepare to respond to security incidents and data breaches."

Michael Bruemmer
Vice President, Experian® Data Breach Resolution

Five Questions for Senior Leadership to Consider on How to bring IT, Physical and Human Security together under a true Information Security Governance Program

As our understanding of these issues evolves, many experts agree that the lion's share of security and privacy risks facing enterprises in 2014 have their origins in human factors vs. technology. This year, if you want to better secure your operations as well as your customers' sensitive data, before acquiring the latest "next generation" security technology cure-all, consider taking a fresh look at how your organization is structured. Here are a few questions to consider:

1. Does your CEO have a company-wide, apples-to-apples view of security risks across all lines of business, or is security oversight and reporting balkanized in multiple stovepipes?

2. Do you have a chief of security with enough authority to set, promulgate and enforce security policy enterprise-wide?

3. Are security and privacy risks included in the portfolio of risk categories monitored and managed by your Chief Risk Officer, or are they managed separately in IT or elsewhere?

4. Has your company developed business-oriented metrics to monitor security posture, gauge the effectiveness of your program over time, and to give the CEO and BoD an accurate understanding of the levels of security and privacy risk they are accepting?

5. Have you established a Security or Security and Privacy Governance Board with senior representation from all lines of business and functional areas? If so, does this board brief the CEO and Board of Directors no less often than once per quarter?

Andy Bochman

CEO, Bochman Advisors

Listing of Key Information Security Areas that Must be Assessed at Least Annually

In support of Data Privacy Day 2014, Loricca recommends that organizations assess, validate and document the strengths and appropriateness of the security controls/safeguards protecting their IT infrastructures and business-critical sensitive data. Key areas of information security that must be assessed at least annually include:

Media Security – protection of all forms of physical storage media including paper documents

Hardware Security – hardware maintenance and change controls, anti-theft, anti-tampering

Software Security – software maintenance and change controls, software integrity, software copyright/licensing compliance, privileged program controls, anti-virus and related malicious software safeguards, database security, security design on new systems

Network Security – network device security, communications security, network access controls, Internet/Web security, intrusion detection, PBX/voice system security, network change controls, firewalls & proxy servers, dialup access security, encryption, e-mail security

Host (System) Security – multi-user and single-user (workstation) computer operating system access controls including: user authentication, data access authorization, audit logs; application security

Procedural Security – information security charter, policies and procedures, organization, roles & responsibilities, auditing, awareness, IT change controls

Personnel Security – background checks, non-disclosure agreements, training, professional development, terminations & transfers, contracts

Disaster Recovery/Business Resumption Planning – Fault tolerance/redundancy, data backup, recovery/continuity planning

Listing of Key Information Security Areas that Must be Assessed at Least Annually

(continued)

Physical Security – facilities access control, security cameras, location and marking of facilities specifically related to impacts to the overall IT infrastructure

Environmental Security – disaster/interruption avoidance, safety, air conditioning and temperature controls, electrical power and utilities

The goal of many companies is to adopt and implement industry-wide standards for acceptable best practices as proffered in ISO 27002 and/or NIST SP 800-53. Additionally, many organizations are required to be compliant with applicable regulatory guidelines (HIPAA, HITECH, PCI DSS, ISO, GLBA, SOX, FFIEC, etc.) and data privacy laws. An important first step in achieving better control over the confidentiality, integrity and availability of sensitive (and sometimes federally protected) business information is to review and update internal policy and procedures for the enterprise, since information security absolutely must be mandated directly from Executive Management. Once sufficient corporate Policies have been established, the workforce must be made aware of how the security policies affect their day-to-day job duties and responsibilities.

Ronald Beltz

Vice President, Loricca

About Cyber Data Risk Managers LLC

CYBER DATA RISK MANAGERS LLC, an Independent Insurance Agency specializes in Data Privacy, Cyber Liability risk, D&O insurance and (IP) Intellectual Property protection. We work with many well known top A-rated Insurance Carriers that specialize and offer insurance coverage for Data Privacy and Cyber Risks as well as (IP) Intellectual Property (Patents, Trademarks & Copyrights).

The team at Cyber Data-Risk Managers LLC is dedicated to helping businesses and organizations find the right insurance policy for their needs. Due to our independent nature, we can help you compare multiple insurance proposals and determine which insurance carrier and insurance policy may work best for your business or organization.

CONTACT:
Christine Marciano,
President/CEO
CYBER DATA RISK MANAGERS
301 N. Harrison Street
Suite 9F, #371
Princeton, NJ 08540
US toll free: 1 +855.CUT.RISK
www.DataPrivacyInsurance.com

We help many different types of businesses and organizations, of all sizes in various industries and sectors create a cyber risk and data breach incident response plan and can also help protect (IP) Intellectual Property. From small-medium sized businesses to health care organizations to critical infrastructure companies concerned about creating a cyber risk and data breach incident response plan, for cloud providers concerned about liability, for technology vendors worried about software patent lawsuits to big retail chains concerned about PCI-DSS and insuring POS-system cyber security risk, we have insurance markets with effective insurance solutions to help mitigate such sensitive risks.

Christine Marciano, President of Cyber Data Risk Managers LLC has over 17 years of Insurance industry experience and is a specialist in Data Privacy and Cyber Risk Insurance.

For cyber/data breach, technology errors & omissions, Directors & Officers and intellectual property insurance solutions and to request an insurance quote, please visit http://databreachinsurancequote.com/cyber-data-risk-managers-products/.