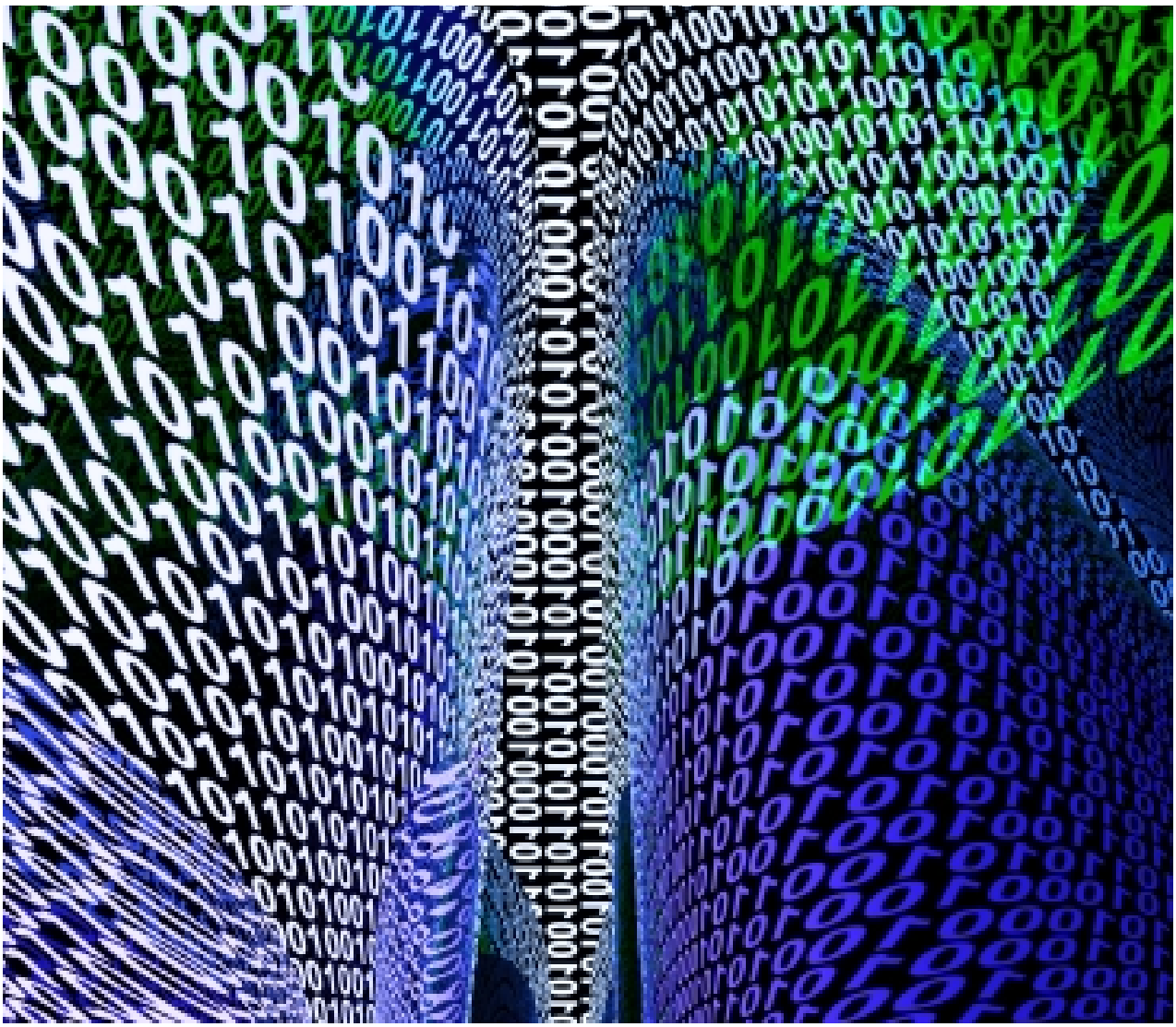
2013 DATA PRIVACY, INFORMATION SECURITY AND CYBER INSURANCE TRENDS



Cyber Data-Risk Managers LLC

www.DataPrivacyInsurance.com

Table of Contents

Authors of the report

James Crowther – Financial Lines Senior Underwriter, DUAL Australia Pty Ltd

Darek Dabbs – CIO, Sera-Brynn

Shaun Dakin – Founder, Privacy Camp / CEO, Dakin & Associates

Anthony M. Freed – Freelance Information Security Journalist

Rebecca Herold – CISM, CISSP, CISA, CIPP, FLMI,
Rebecca Herold & Associates, LLC aka The Privacy Professor

Rick Kam – CIPP/US, President and Co-Founder, ID Experts

Charles Kellenbach – General Counsel and Chief Legal Officer, Heartland Payment Systems

Christine Marciano – President, Cyber Data Risk Managers

Aaron I. Messing - Information Privacy Attorney, OlenderFeldman LLP

Erwann Michel-Kerjan - Managing Director, Risk Management and Decision Processes Center and Adj. Associate Professor, Operations and Information Management Department, Wharton School of Business

Matthew Negus –Associate, Promontory Financial Group LLC

William Oravecz – Healthcare Informatics & Management Consultant and Managing Partner and Chief Consultant at WTO Associates LLC, New Haven, CT

Dr. Larry Ponemon – Chairman and Founder, Ponemon Institute

Richard Santalesa – CIPP/US, Senior Counsel, InfoLawGroup LLP

Hilary Schneider – President, LifeLock

Bruce Schneier – Security Guru, Internationally Renowned Security Technologist and Author

Jody Westby – CEO and Founder, Global Cyber Risk LLC

2013 Data Privacy, Information Security and Cyber Insurance Trends Report

Introduction by

Christine Marciano, President, Cyber Data Risk Managers LLC

To help show our support of Data Privacy Day 2013 and the importance of "Data Privacy and Security risks," Cyber Data Risk Managers chose to release its 2nd Annual Data Privacy, Information Security and Cyber Insurance Trends report on Data Privacy Day 2013. We have quite an impressive lineup of recognizable industry experts that we have selected to be in this *exclusive* and one of a kind report. We're confident that you will enjoy reading this report just as much as we have greatly enjoyed putting it together.

We went all out this year and asked top industry experts their thoughts on what they think, feel and should happen in 2013 and what steps can be taken to mitigate data privacy and security risk. Taking a bold approach, we even asked several experts for their thoughts on the good, bad and ugly of "why organizations *may or may not* be rushing to purchase cyber insurance."

Beyond embarrassment, today the private and public sectors face financial and reputational damage, competitive inroads, and significant regulatory sanctions when confidential information is inadequately protected. Clearly enough reasons as to why cyber security must be prioritized regardless of what sector one conducts their organization.

As our nation has become heavily reliant on the internet, organizations, public and government agencies and businesses of all sizes continue to struggle with cyber security due to the continuous force and increasingly sophisticated cyber threats that have become the new norm. Intrusion prevention suppliers reveal privately that their systems are unable to keep up with the sophistication of attacks, and anti-virus companies report that attackers are reverse-engineering the vendors' antivirus software and building new viruses so sophisticated that the tools cannot stop them.[1] At the time this report was published, it was reported that the hacktivist group, Anonymous had taken over the website of the U.S. Justice Department's Sentencing Commission and threatened to release sensitive government data and use computer-code based "warheads" against other sites. Simultaneously, U.S. financial institutions are being pounded with high-powered cyber attacks that some suspect are being orchestrated by Iran.

[1] F-Secure presentation, May 21, 2008, IMPACT Launch at the First World CyberSecurity Summit, Kuala Lumpur, Malaysia.

Besides the weekly round, or of late what seems to be becoming more of a daily occurrence of cyber attacks just as much continues to happen offline as well. "Unencrypted" mobile devices continue to get lost which in turn increases the number of data breaches that we all read about in the media headlines on what seems like a weekly basis.

Inadequate security measures on government and private sector networks, critical infrastructure and telecommunications represent perhaps the most potent national security and economic risks facing the nation. There also seems to be a disconnect and an element of collaboration[2] missing between the Federal Government and the private sector as it pertains to cyber security. Teamwork is essential to getting things done. In todays global and digital 24/7 world, challenges are more complex; it's becoming increasingly important to bring more, diverse minds to the table and to break down silos.[3]

When you think about our digital society and how our lives and businesses are lived and conducted online and how our critical infrastructure has become reliant on the internet and with "Big Data" and the (IoT) "Internet of Things"[4] getting into more conversations, it is quite unsettling that yet there is a looming lack of security in protecting and guarding the security of our critical infrastructure, (PII) personal Identifiable information, (PHI) personal health information and intellectual property. Imagine if you lived in a city that had a high crime rate, would you feel comfortable at night leaving your door unlocked and not having a security system in place to alert you of an intruder? Of course not. However, the private sector along with the public sector has not displayed a strong commitment to cyber security, to put it mildly.

In my opinion, "smart regulation" along with "smart incentives" must occur in 2013. There needs to be a focus on real-time information sharing. As Albert Einstein said ever so brilliantly "Insanity is doing the same thing, over and over again, but expecting different results." This can no longer be tolerated as it pertains to cyber security. We must work to understand what the threat actor is doing and how to disrupt it. Perhaps for starters, we need to start thinking like an attacker and maybe we will see different results.

As I was preparing this report, I had some great discussions with several industry experts that are included in this report and the census is that "Data Privacy" is something that all of us can agree must be safeguarded and protected. With that being said, 2013 could ultimately become the year that "Data Privacy and Cyber Security" reaches groundbreaking levels. Congress has recently stated it's a priority this year to act on comprehensive cyber security legislation and

[2] NIST Invites Institutions to Join National Cybersecurity Excellence Partnerships, http://csrc.nist.gov/nccoe/ncep_frn_announcement_oct-19-2012.html

[3] The Four Key Elements of Innovation: Collaboration, Ideation, Implementation and Value Creation, http://www.stlouisfed.org/publications/br/articles/?id=1029

[4] The Internet of Things Has Arrived — And So Have Massive Security Issues, Wired.com, http://www.wired.com/opinion/2013/01/securing-the-internet-of-things/

has introduced a new Bill called the "Cyber Security and American Cyber Competitiveness Act 2013."[5]

Many other countries are also taking steps in the right direction to ensure that Data Privacy and Cyber Security are of utmost importance. Australia's Prime Minister Julia Gillard recently announced that a new Australian Cyber Security Center (ACSC) will be established in Canberra to boost the country's ability against cyber-attacks.[6] The European Union also continues its talks on its proposed Data Protection Regulation and Directive.

The threat environment going forward is likely to evolve and become even more sophisticated. Perhaps more attention and focus should be on mitigating their impacts through proactive coordinated response plans and effective information sharing.

The good news is that due to what's become the new norm of cyber attacks, threats and data breaches our nation's private and public sectors have become more increasingly aware of the wide range of exposures we're faced with as it pertains to lost or stolen data, violation of privacy laws, intellectual property infringement, social media, mobile devices, (BYOD) Bring Your Own Device and cloud computing. With a new year upon us, 2013 is setting up to be quite an interesting year as it pertains to "Data Privacy and Cyber Security." It should come as no wonder then that many in the private and public sectors will turn to Data Breach/Cyber Insurance as a way to mitigate the residual risks of a security incident and/or a data breach.

A recently conducted Zurich survey[7] stated that as awareness grows, information security and cyber risk continues to represent at least a moderate threat for a majority of risk professionals, who more and more are adopting an enterprise-wide approach to information security and cyber liability risk management. Due to improved awareness, cyber insurance also is increasingly becoming a part of more organizations cyber risk management strategies.

We all know that life offers no guarantees and that "when one door closes, another one opens." This holds true for cyber security, especially with today's evolving threat environment and the force of attacks that continue to knock on the doors of countless networks.

Enter "cyber insurance." While cyber insurance cannot stop incidents or prevent them from happening, it can help respond to incidents when they do happen. When a security incident or a data breach happens, most cyber insurance policies have a team of experts already in place to

---

[5] http://commerce.senate.gov/public/?a=Files.Serve&File_id=b678eb9a-b5c1-4540-aca3-3e857c7627da

[6] Strong and Secure: A Strategy for Australia's National Security, http://commerce.senate.gov/public/?a=Files.Serve&File_id=b678eb9a-b5c1-4540-aca3-3e857c7627da

[7] Information Security, Cyber Liability & Risk Management: The Second Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management, by Zurich, http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/zurich_2012cyber_surveyreport.pdf

help determine how your incident happened, whether or not any sensitive (PII) Personally Identifiable Information or (PHI) Personal Health Information has been exposed and helps determine if the security breach needs to be reported. Cyber insurance offers the private and public sector the ability to mitigate the residual risk, losses and associated costs of a security incident and/or data breach. Cyber insurance protects against the liability that comes from compensating others because cyber security has failed.[8]

Cyber insurance, aka "privacy and security" insurance continues to evolve as many more businesses, organizations and risk managers are realizing that it can be used as a way to respond to a data breach and/or security incident and as a key component of an incident response plan.

While cyber insurance has been around for 10+ years, it is only within the last few years that more policies have come to market. It remains a specialized product, which should naturally require working with a specialist. Would you ask your General Medical Doctor for specialized advice on a health threat he does not follow or practice? Of course not This same theory applies to cyber insurance. A cyber insurance specialist understands the evolving cyber risks and threats that private and public sectors face and can help customize a cyber insurance policy based on what coverages may or may not be needed. With over 30+ cyber insurance carriers today offering non-standard policies, a broker specializing in cyber insurance can help make what's been stated as a difficult process become an easier and informative process.

We here at Cyber Data Risk Managers will continue to spread the word that all Data Breach/Cyber Insurance policies are different and that working with a cyber insurance specialist should be a minimum requirement when exploring the purchase of such a specialized insurance policy. As specialists in Data Breach/Cyber Insurance, we will continue to lead the way and help build awareness of how cyber insurance can help the private and public sectors mitigate the residual risks and costs associated with a security incident and/or data breach.

At Cyber Data Risk Managers, we work to understand not just the various Data Breach/Cyber Insurance policies that are available today, but also the threats of today and the trends of tomorrow. That helps us to help you better understand and protect the risks that surround your sensitive and confidential data assets.

We're big strategic thinkers here at Cyber Data Risk Managers so naturally we have aligned ourselves with some pretty big industry experts who share similar interests and goals in seeing

[8] It's important to note that cyber insurance policies are non-standard policies and vary by insurance carrier. For specific policy coverages, endorsements and limitations, seek the advice of an insurance broker specializing in cyber security insurance who can help your organization navigate the various policies and coverages that are available.

that “Data Privacy and Cyber Security” is brought to the forefront of the 2013 agendas of those who can make an impact and big change happen.

Our 2013 agenda here at Cyber Data Risk Managers is not to impress but to be at the forefront and continue to be on the pulse of building cyber insurance awareness and to help improve and bring change to the market where it’s needed. Big change requires big goals and we’re confident that through our alignment and collaboration with big industry, government and academia experts we can accomplish our big goals. Stay tuned.

I sincerely appreciate and would especially like to thank all of those who have contributed to this report. I’m truly amazed and feel honored by what they have shared with us. Their contributions offer many insightful views of the 2013 Data Privacy, Information Security and Cyber Insurance landscape relevant to businesses and organizations of all sizes and sectors.

It’s my hope that you find this report not only interesting, but helpful in making 2013 a safe and secure year. If you would like to learn more about how you can help improve and bring change where it’s needed as it pertains to 2013 Data Privacy, Information Security and Cyber Insurance I welcome you to contact me.

Christine Marciano
President, Cyber Data Risk Managers

Follow Christine on Twitter:
@DataPrivacyRisk

Bruce Schneier – Security Guru, Internationally Renowned Security Technologist and Author

When it comes to security, we're back to feudalism[9]. Today's internet feudalism, however, is ad hoc and one-sided. We give >companies our data and trust them with our security, but we receive >very few assurances of protection in return, and those companies >have very few restrictions on what they can do. This needs to change. There should be limitations on what cloud vendors can do >with our data; rights, like the requirement that they delete our data when we want them to; and liabilities when vendors mishandle our data.

[9] When It Comes to Security, We're Back to Feudalism, Bruce Schneier, http://www.schneier.com/essay-406.html

James Crowther – Financial Lines Senior Underwriter, DUAL Australia Pty Ltd

The recent Bill that passed on the 29th November 2012 was the first part of the Federal Governments response to Australian Law Reform Commission's (**ALRC**) 2008 Report on Australian Law and Practice. One of the recommendations in the ALRC's report was to introduce a mandatory data breach notification scheme. The Federal Government did not respond to this recommendation in the first part of its response but it will be next on the agenda. To highlight this, the Federal Attorney-General has released a Discussion Paper seeking comment on whether to introduce laws to make notification of data breaches by government agencies and large private sector entities mandatory in Australia.

In the meantime notification is voluntary, as is best practice given that organisations are still 'highly recommended' to comply with OAIC's Guide - Data Breach Notification: A Guide to Handling Personal Information Security Breaches, that was first introduced in 2008.

With the costs of a data breach in Australia increasing from $128 (2010) to $138 (2011) per record (according to research released by Symantec), the cost to organisations can be significant. The Australian insurance market has seen a number of policies launched to provide a solution for these type of incidents that are on the rise, amongst others.

It is important as always to read the policy wording carefully, as some policies can be deficient in responding to certain breaches. The DUAL Australia Cyber & Privacy Protection Policy is a comprehensive six module policy, the Breach Costs Module offers cover for a large range of breach notification costs but importantly it offers broad language in responding to; voluntary notification costs as well as mandatory notification costs, and also covering a breach of personally identifiable information held by anyone on the organisations behalf.

Looking ahead into 2013, Australian organisations should need to consider how they will respond to these changes in legislation and prepare themselves for the very real possibility of the Federal Government introducing mandatory data breach notification laws.

Darek Dabbs – CIO, Sera-Brynn

Question: Why do you think the organizations that you work with are not rushing to purchase cyber insurance? Especially when data breach costs continue to increase and cyber insurance can help cover the residual costs?

During the year 2013, businesses can expect to see significant increases in Cyber Threats and successful attacks due to the proliferation of underground hacking toolkits. Traditionally, a skilled hacker is required to do significant research and customize individual vulnerability exploits against targeted networks. However, the battlefield is rapidly changing. What worked to keep a business safe yesterday is not going to be up to the task tomorrow. The newest hacking toolkits are designed in such a simplistic nature that any unskilled adversary can download a hacking toolkit and blindly point and click a few buttons to automate complex and powerful attacks against multiple targets.

Historically, many businesses were simply not affected by skilled hackers because of their size and the difficulty associated with successfully bypassing their defenses. Today, anyone on the Internet is a target for these junior hackers utilizing the newer advanced automated toolkits. The toolkits themselves are being updated and upgraded with zero-day vulnerability exploits faster than business software developers can remediate and patch the vulnerabilities. This leaves business networks at a severe risk of Data Breach and network outages. Organizations that expect internal non-security focused system administrators and IT support staff to defend against those threats place themselves in a reactive posture instead of a more cost-effective proactive approach. The costs incurred from a Data Breach event far outstrip the cost of a proactive Cyber Security approach. Unfortunately, many businesses currently think a breach will never happen to them – and this is precisely the attitude hackers are depending on. In 2013, we can expect to see some of those businesses close their doors due to the crippling costs of fines, litigation, and remediation associated with successful Cyber Attacks.

Shaun Dakin – Founder, Privacy Camp / CEO, Dakin & Associates

I'd say that the major trend for organizations is BYOD and the data security and privacy risk that comes with that. Employees are demanding that they have their own iPhones, Androids, Tablets, etc.. at work and even if they are not company issued, there is nothing that can stop them from bringing their own device into their work.

Employees will use these devices mostly to keep in touch with friends and family but will be conducting social media (tweets, facebook updates, photos, etc...) which could put your company at risk.

Short of banning people from bringing their own devices into the office building, ongoing education and training is critical to make sure that your employees understand what they can and can not do with their BYOD.

Follow Shaun Dakin on Twitter:

@ShaunDakin

@PrivacyCamp

Anthony M. Freed – Freelance Information Security Journalist

Enterprises need to be aware of an increase in malware designed to evade detection by the automated detection systems their antivirus providers use to help evaluate the millions of new samples of potentially malicious code examined on a daily basis. The automated systems employ a virtual environment where the code samples can be safely evaluated. The problem is that clever malware developers are increasingly using system "hooks" that leave the malicious code dormant until an end user triggers their functions with a keystroke or mouse click, for example. Given that the automated detection systems do not use external hardware such as a mouse or keyboard, these types of malware are being overlooked and subsequently not being added to the list of known agents in antivirus software updates. Similar to how attackers may use zero-day exploits in targeted campaigns consistent with Advanced Persistent Threats, these types of detection-evading malware may become more prevalent in spear-phishing operations aimed at high value targets. Continued focus on employee awareness and security education is vital to decreasing the chance that enterprise information systems will be infected by these agents.

Follow Anthony M. Freed on Twitter:

@anthonymfreed

Rebecca Herold – CISM, CISSP, CISA, CIPP, FLMI,
Rebecca Herold & Associates, LLC aka The Privacy Professor

One of the biggest privacy risks that exists, and that is not actively or effectively addressed often enough, is outsourcing the storage, processing, or any other type of access, of information that contains personal information. I find a report of a privacy breach or security incident every week, and often literally every day. Historically organizations that outsourced information processing only addressed the issue of having the outsourced entity to secure the information by including a clause in their contract, or often, trying to simply relieve themselves of any liability for any bad things that happened to their data when it was in the hands of their outsourcer. In the past few years we have seen the number of breaches that are occurring within business partners, particularly with those who are business associates under HIPAA, increasing dramatically. We've also seen the sanctions against the organizations who outsourced to those entities increasing, in frequency and in severity.

I anticipate 2013 will see a drastic increase in not only breaches occurring within business associates and other types of business partners, but also the sanctions for the organization that did the outsourcing will increase, and the contracted entities are going to start receiving sanctions as well. To mitigate the risks that business partners bring along with their services, organizations need to do more than just include a short clause in their contracts with business partners. They need to:

1) Provide details for specific information security and privacy activities within the contracts that the business partner must do to safeguard their data.

2) Require regular validation from the business partners that they are following their information security and privacy program, and keeping it updated appropriately. I have found a couple of methods work well for this:

a. Require the business partner to fill out a monthly attestation that covers their security and privacy compliance activities, and requires the CEO (or other accountable executive) to sign his or her validation that the activities actually occurred. I create these for several of my clients, and I also include a quiz, that varies each month, that the business partner has to complete to demonstrate their understanding of information security and privacy concepts.

b. Require access, upon request, to review the business partner's policies and supporting compliance documentation. There are many ways to accomplish this, in addition I created a service to make this as simple as possible for both the organization and their business partners.

3) Require the business partner to provide regular training and ongoing awareness communications to their staff that are involved in providing their services and accessing the

data. Require them to provide documentation that validates such training and awareness upon request.

4) Maintain an up-to-date inventory of all business partners, that includes the contact information for the primary account representative and also a list of all the types of personal information, as well as sensitive information as applicable, that the organization has entrusted to them. I like to also see organizations take a few hours each month to do a quick online check of their business partners to see if they have been involved in any privacy breach or security incident. The organization can then get in touch with them to see how the event may have impacted, or could impact, the organization's information.

5) Ensure the organization contractually requires the business partner to have a documented, detailed breach response plan. Then, ensure the organization coordinates with the business partner to do regular (such as annual) breach response plan tests/run-throughs. Be sure to document the different types of breaches that may occur, how quickly the business partner will contact the organization for each type of breach, the information the business partner needs to provide to the organization in such events, and the breach notice roles and responsibilities.

Follow Rebecca Herold on Twitter:

@PrivacyProf

Rick Kam – CIPP/US, President and Co-Founder, ID Experts

"Data breaches are now part of doing business. To help address this,organizations need to operationalize pre-breach and post-breach processes," said Rick Kam, president and co-founder of ID Experts.

"Looking ahead to 2013, organizations should also update their policies and procedures to include mobile devices and cloud, since these pose high risk areas for data."

Follow Rick Kam on Twitter:

@RickKam

Charles Kellenbach – General Counsel and Chief Legal Officer, Heartland Payment Systems

<u>Question:</u> Why do you think the organizations that you work with are not rushing to purchase cyber insurance? Especially when data breach costs continue to increase and cyber insurance can help cover the residual costs.

Looking at this from the consumer side and having acquired cyber insurance ourselves, I understand that there is value to purchasing a cyber insurance policy. However, while around for a number of years, cyber insurance is still a fairly new and evolving market. When our merchants are breached, many are harmed financially and some even go bankrupt as they are not able to handle the punitive fees that are assessed against them. There could be some value for our merchants to purchase a cyber insurance policy. However, the whole purpose of purchasing a cyber insurance policy is to cover a data breach when one occurs. I can't stress enough how important it is for a prospective policy buyer to do their due diligence and learn the policy limitations and what is or what is not covered under the policy. It would be wise and of great value for a prospective buyer to work with a sophisticated cyber insurance broker who has expertise in this product. In my experience, I find there is often a disconnect between what one thinks should be covered under the policy and what is actually covered. A prospective buyer needs to be educated and informed about what is and what is not covered under the policy before purchasing coverage. Otherwise, the potential of coverage being there when needed might turn into a court battle. That's not something any insured wants to be bothered with at the same time they are experiencing a data breach.

Aaron I. Messing - Information Privacy Attorney, OlenderFeldman LLP

2012 was notable for several high-profile breaches of major companies, including LinkedIn, Yahoo!, and Zappos, among others. As businesses move more confidential and sensitive data to the cloud (especially in the aftermath of Hurricane Sandy's devastation and the havoc it wreaked on businesses with locally-based servers), data security obligations are of paramount importance. Businesses should expect more notable data breaches, more class-action lawsuits, and federal legislation concerning data breach obligations in 2013.

To protect themselves, business should: (i) require that cloud providers and other third-party vendors provide them with a written information security plan containing appropriate administrative, technical and physical security measures to safeguard their valuable information; and (ii) ensure compliance with those obligations by drafting appropriate contractual provisions that delineate indemnification and data breach remediation obligations, among others. In particular, when using smaller providers, businesses should consider requiring that the providers be insured, so that they will be able to satisfy their indemnification and remediation obligations in the event of a breach.

Follow Aaron Messing on Twitter:

@amess

Erwann Michel-Kerjan - Managing Director, Risk Management and Decision Processes Center and Adj. Associate Professor, Operations and Information Management Department, Wharton School of Business

Question: What do you think is the biggest risk to organizations today and what can they do to mitigate their risk in 2013?

"Pretend cyber-risks will not happen to them. Organizations need to go beyond the reassuring assumptions that they are safe and seriously test the robustness of their systems. To do it well will cost time, money and require expertise, but this might be the best investment to be made in 2013"

Question: Looking ahead into 2013, what do you feel we can expect to see happen and what can be done to mitigate risk?

"The number of attacks against small and big brand is going to continue to increase; attacks on some of your key suppliers or customers can be very damaging to your bottom line too so establishing collaborative ways to mitigate risks is critical. This is done by approaching cyber-risks in a more system-based manner rather than looking at each risks in silo: there are massive interdependencies out there."

Question: Why do you think organizations may or may not be rushing to purchase cyber insurance? Especially when data breach costs continue to increase and cyber insurance can help cover the residual costs.

"What is important is for firms to work with their insurers to develop products that add value to the firm, not simply buy the latest product on the market because it's trendy. Insurance must be tailored. In other words, be smart"

***** Christine Marciano sends a special thank you to Professor Michel-Kerjan for taking the time out of his busy schedule to write this contribution as he was in the middle of preparing for the start of Davos 2013 when he wrote this contribution.*****

Matthew Negus –Associate, Promontory Financial Group LLC

Towards the end of 2013, the text of the proposed General Data Protection Regulation is likely to be finalised within the machinery of the European Commission, following which there will be a lead time of 2 years to allow EU member states to ready themselves prior to full implementation. The regulation includes a number of sweeping changes to the existing regime which may include the introduction of mandatory notification of personal data security breaches to regulators (within 24 hours) and to data subjects (as soon as is practicable).

Whilst it is likely that there will be some changes to the current text of the regulation, it is widely expected by industry experts that the proposals regarding mandatory breach notification will remain. Voluntary breach notification is recommended by many data protection authorities across Europe, and is mandatory amongst telecommunications providers. However, this is likely to represent a step into the unknown for many organisations and particularly those within industry sectors which are not accustomed to a significant regulatory regime.

Although the European cyber risk and data breach insurance market is still in its infancy there is likely to be an increase in take-up once the text of the regulation has been finalised. In particular, this is likely to be most prevalent amongst small/medium-sized firms looking to remove the risk of incurring costs associated with breach notification from their balance sheet. Organisations should, nonetheless, take appropriate steps to ensure they have a demonstrable compliance framework in place. Cyber risk and data breach insurance should not be used as a substitute for investing in risk management.

William Oravecz – Healthcare Informatics & Management Consultant and Managing Partner and Chief Consultant at WTO Associates LLC, New Haven, CT

Question: In looking back at 2012, cyber attacks and data breaches are an almost daily occurrence. As it pertains to Data Security and Data Privacy, what do you think is the biggest risk to organizations today and what can they do to mitigate their risk in 2013?

Not having a dedicated IT security team/consultant, comprehensive Security Risk Analysis and Security Asset Inventory in place.

Best bet is to hire a certified HIPAA/HITECH and IT Security consultant to if not jump start your program, but to have an expert outsiders opinion and recommendation of where you stand and what is a priority. Money spent up-front will save far more than money spent to remediate a breach.

Question: Looking ahead into 2013, what do you feel we can expect to see happen and what can be done to mitigate risk?

More focus will be placed on security infrastructure and process improvements by healthcare providers.

Engage a HIPAA/HITECH certified Consultant to ensure you are doing the right things at the right cost.

Question: Why do you think the organizations that you work with may or may not be rushing to purchase cyber insurance? Especially when data breach costs continue to increase and cyber insurance can help cover the residual costs.

Many healthcare providers are unaware of cyber security insurance. They are not thinking of the big picture. Organizations need to appreciate that both technical AND FINANCIAL RISK needs to be addressed for their IT infrastructure. Just like one purchases homeowners' insurance or motor vehicle insurance. You need to be prepared for the low likelihood-high impact threat that may strike despite your best HIPAA/HITECH IT security preparation.

Follow William Oravecz on Twitter:

@WTOAssociates

Dr. Larry Ponemon – Chairman and Founder, Ponemon Institute

<u>Question:</u> Why do you think the organizations that you have interviewed through your research are not rushing to purchase cyber insurance? Especially when data breach costs continue to increase and cyber insurance can help cover the residual costs.

"Our research shows healthcare providers such as hospitals and clinics are late adopters when it comes to investments in data protection and information security. This is probably true for cyber insurance as well," said Dr. Larry Ponemon, chairman and founder, Ponemon

Richard Santalesa – CIPP/US, Senior Counsel, InfoLawGroup LLP

Costly high-profile cloud vendor outages in 2012 drove home for Enterprise IT and C-Level executives that the status quo for cloud Service Level Agreements can't continue in 2013. As the National Institute for Standards and Technology (NIST) moves toward completion of cloud recommendations, in step with the growth of cloud brokers and third-party cloud security accreditation, cloud vendors will increasingly quietly relent in accommodating increased limits on liability for downtime and breaches above the current standard of providing mere service "credits." Legal teams negotiating cloud contracts therefore should continue to press for meaningful cloud SLAs while working with their insurance professionals to ensure existing cyberrisk and business disruption coverages match the new data security realities in the move toward cloud storage onramp and growing hybrid cloud implementations.

Follow Richard Santalesa on Twitter:

@richnet

Hilary Schneider – President, LifeLock

<u>Question:</u> What do you think is the biggest risk to organizations today and what can they do to mitigate their risk in 2013?

"One of the biggest risks any organization faces today is preventing a breach of their data. This type of data theft can happen from any spot on the globe with an internet connection. Having a comprehensive information security plan that is followed at all levels of the organization is an imperative."

<u>Question:</u> Looking ahead into 2013, what do you feel we can expect to see happen and what can be done to mitigate risk?

"I believe that 2013 is going to be the year of the mobile breach. With the increase in quantities of mobile devices from your smartphone to your tablet, there are increased opportunities for information to be stolen. Think of your mobile device as your passport or the keys to your house. Keep it locked and secure when not in use and ensure that all security precautions are taken during use."

Jody Westby – CEO and Founder, Global Cyber Risk LLC

Question: What do you think is the biggest risk to organizations today and what can they do to mitigate their risk in 2013?

I anticipate that privacy will be a banner issue in 2013. The Administration and FTC can be expected to continue their push toward a legal framework that is more compatible with the EU's Data Protection Directive. Congress also will attempt to push through some sort of cybersecurity legislation. This will cause 2013 to become the year that privacy and security finally get the attention of business executives, as they begin to realize the enormous impact that such legislation will have on their business processes, IT systems, and budgets.

Question: Looking ahead into 2013, what do you feel we can expect to see happen and what can be done to mitigate risk?

Looking forward into 2013, until cybercrime gets confronted and addressed, cyber attacks will become more sophisticated and intellectual property and corporate data will continue to be the prime targets. Whenever there's the opportunity to make money on stolen data without getting caught, you can bet there's going to be more hackers, malware schemes, and major data breaches.

Question: Why do you think the organizations that you work with may or may not be rushing to purchase cyber insurance? Especially when data breach costs continue to increase and cyber insurance can help cover the residual costs.

My view on cyber insurance is that it is an evolving and growing market and organizations still don't understand the categories of available coverages that are being offered today. Risk managers are concerned about what is and what is not covered and most are not sure if they even need to purchase this type of coverage. The more they seek solutions that will give them valuations on cyber risks, the better equipped they will be to understand the ROI on security programs and the business exposure costs they need to cover with insurance coverage.

CYBER DATA RISK MANAGERS LLC, an Independent Insurance Broker that 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, helping compare multiple insurance proposals and determining which insurance carrier and insurance policy may work best.

Cyber Data Risk Managers works to understand not just the various Data Breach/Cyber Insurance policies that are available today, but also the threats of today and the trends of tomorrow.

While cyber liability insurance policies vary by insurance carrier, some of the coverage offerings that Cyber Data Risk Managers offers include (not limited to):

- Network Security coverage
- Data Breach Incident Response coverage
- Multimedia Liability
- Cyber Business Interruption
- Cyber Extortion
- Hacker Damage
- Litigation/Enforcement Proceedings
- Third Party Systems

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.

CONTACT:

Christine Marciano, President
CYBER DATA RISK MANAGERS LLC
301 N. Harrison Street, Suite 9F, #371
Princeton, NJ 08540-3512 USA
US toll free: 1 +855.CUT.RISK
Fax: 1 +732.709.1684
www.DataPrivacyInsurance.com
Email: CMarciano@DataPrivacyInsurance.com
Twitter: @DataPrivacyRisk