2012
DATA PRIVACY AND INFORMATION SECURITY PREDICTIONS

Cyber Data-Risk
Managers LLC

This is our first Data Privacy and Information Security Predictions report. We asked leading Data Privacy and Information Security professionals what they thought the New Year will hold in terms of the threats that are on the 2012 landscape. The predictions that are included in this report offer a wide range of threats and concerns that need to be considered by every business or organization that operates in cyberspace regardless of its size.

As we start 2012, we can expect to see a continuance of data breaches and increasing cyber attacks. Taking a look back at 2011, we have learned that no system is ever 100% secure no matter the name or the size of an organization. It's important for businesses and organizations to know what they need to be prepared for and to take steps to help minimize the threats that do not appear to be going away.

Looking ahead, it appears that in 2012 we will see an increase of heightened and very sophisticated threats than what was seen in 2011. We can recall 2011 as the year the hackers and the hacktivists got started on the data breach and gained a great amount of attention. With all of the digital information and big data that is being stored, it should come as no surprise that data breaches are not going away in 2012 as they are only going to get bigger. I expect that we will also see more serious hacktivists attacks. It seems that the hacktivist is no longer hacking organizations just for the fun of it. They are attacking for specific causes and I believe that hacktivists are going to be a very serious threat in 2012 and organizations must be prepared.

I fear that the attention that was given to the data breach in 2011 may diminish being that the data breach will become commonplace in 2012 and going forward. Whether a data breach makes the front page news is not the point. All businesses and organizations must take a data breach seriously. I sincerely hope that legislation is passed early this year that will dictate exactly how seriously businesses and organizations must take a data breach.

I also feel that "Big Data" is something all of us need to be concerned about. Big Data that is stored by various data holders includes details on almost everything all of us do when we are plugged in. We will begin to see many organizations moving their big data into the cloud. Big Data stored in the cloud is a huge risk if it's not properly secured. I predict that we will begin to see enhanced cloud security due to the Federal Agency IT moving a great deal of its data into the cloud (they will hopefully pave the way for cloud security).

It's also my hope that consumers start realizing that they need to stand up and fight for their right to privacy and to stop living their lives so publicly online. Today it is very easy for an Identity Thief to piece together an entire puzzle of our lives from all of the information that is available and collected about us online. Much of this information is from consumers who willingly share this data without being compensated.

I also predict that we will see a higher amount of businesses and organizations start planning for the eventuality of a data breach as today most realize that it's not a matter of "if" a data breach will happen, it's a question of "when?' When a data breach happens, businesses and organizations are beginning to realize that it's best to have a plan of action ready and in place. This leads me to predicting that "Data Breach/Cyber Insurance" is positioned for a sizable increase in growth in 2012. Many organizations will turn to Data Breach/Cyber Insurance in order to create a data breach response plan in preparation for a data breach and/or cyber attack.

We here at Cyber Data Risk Managers will continue to spread the word that all Data Breach/Cyber Insurance policies are different. As specialists in Data Breach/Cyber Insurance, we will continue to lead the way and help businesses and organizations navigate the various policies that are available and help determine which is best for their needs.

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 protect your data and assets.

I sincerely appreciate and would like to especially thank all of those who have contributed to this report.

I hope that you find the predictions that follow to be not only interesting, but helpful in making 2012 a safe and secure year.

Christine Marciano
President, Cyber Data Risk Managers

Follow Christine on Twitter:
@DataPrivacyRisk

SMARTPHONES AND INTERNATIONAL CYBERCRIME

Misha Glenny, **Author of *DarkMarket: Cyberthieves, Cybercops and You.* (Knopf, 2011) states…**

1) It would be churlish to ignore the problems posed by smart phones, especially in the light of the spate of attacks on the Android system. In terms of the mass market, this must represent the greatest challenge for the security industry.

2) They won't go on the record about it for reasons of political correctness but cyber law enforcement officers all dread the anticipated proliferation of hand-held devices in Africa as this is likely to trigger a significant increase in 419 style frauds and other online crimes. I would like to stress, however, that the positive aspects of Internet proliferation in Africa far outstrip the negative ones.

3) I suspect that the Chinese authorities are becoming genuinely concerned about crime on the web and that there will be moves toward a more coordinated approach to security between the West and other major Internet powers as the threats from state and non-state actors alike proliferate.

Follow Misha Glenny on Twitter:
@MishaGlenny

CYBERINSURANCE IS POSITIONED FOR REAL GROWTH IN 2012

Jim Duster, Vice President of Sales, Debix , says…

"We're seeing a trend of organizations that have experienced a data breach transferring risk to insurance carriers to better manage cost associated with these incidents."

Follow Debix on Twitter:
@AllClearID

Jake Kouns, Director of Cyber Security and Technology Risks Underwriting, Markel Corporation, says…

"Many people may find it fun to release security predictions for the coming year, but the reality is most of them are complete guesses."

What we do know is that 2011 was an extremely active year for data breaches. DatalossDB.org tracked 841 incidents as of 12/9/2011, a 37.4% increase over all of 2010. Three incidents in 2011 have been added to the Top 10 all time 'records lost' list and that does not even include Epsilon, as it is still an unknown amount of records. It doesn't take a fortune teller to predict that we can expect more of the same in 2012, including new privacy regulations being proposed as well as an increasing number of lawsuits aimed at companies that suffered a breach. With real exposures, companies should seriously evaluate transferring a portion of their risk by obtaining Cyber Liability insurance.

Follow Jake Kouns on Twitter:
@Jkouns

DATA BREACHES WILL FORCE MANY TO REVIEW THEIR EXISTING INSURANCE POLICIES TO SEE WHAT'S COVERED

Scott N. Godes, Counsel, Dickstein Shapiro LLP, states…

In terms of a trend in the areas of privacy and information security, I have noticed a sea change in both areas, leading to more need for analysis of insurance policies to cover these risks. When considering privacy risks, there has been an expansion of risks and potential liability for privacy violations, with the *Pineda v. Williams Sonoma* decision serving as one example. This year also has been called the year of the data breach, and companies are taking a hard look at how their insurance might and does cover such claims. These risks are being considered much more closely by companies, along with a careful analysis of how their insurance policies might cover.

Follow Scott Godes on Twitter:
@insurancecvg

→ EU DATA PROTECTION REGULATION CHANGES
→ HIPAA BREACH NOTIFICATION CHANGES
→ UPCOMING FTC PRIVACY REPORT
→ CLOUD COMPUTING

InfoLawGroup Senior Counsel, Richard Santalesa predicts…

Even though 2011 was an extremely active year on the information security and privacy fronts – with a blizzard of proposed legislation, near weekly front page data breaches and the continued full leap into the cloud with its securities issues – I predict that 2012 events across the privacy and data security landscape will make 2011 look like a casual Sunday walk in the park. A handful of thoughts on what 2012 may hold:

The EU's on deck Data Protection Regulation promises – or threatens depending on your viewpoint – to significantly revamp the EU's data protection regimes and adding potential uncertainty to the EU arena. The leaked DPR indicates movement toward a new broad extraterritorial reach, stronger protections for children under 18, firm embrace of privacy by design and the right to be forgotten, a requirement to designate a privacy officer and increased enforcement powers and penalties. We'll see what happens when the rubber actually meets the road in 2012.

Will the final version of the HIPAA breach notification rule make a long-awaited appearance in 2012? The smart money says yes, especially since Congress recently admonished DHS to hurry up already given that the "interim" rule has been around since 2009. We may also see guidelines issued per Stage 2 of the electronic record incentive program within the HITECH Act.

The FTC front and center. The FTC plans in early 2012 to issue its finalized Privacy Report, formally titled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," which I believe will have significant impact on the 2012 privacy/infosec landscape. The draft version, released a year ago in December 2010, immediately sparked wide-ranging conversations on

(continued) InfoLawGroup Senior Counsel, Richard Santalesa

Do-Not Track, Privacy by Design, Fair Information Practice Principles, Geolocation and other privacy-related issues, many of which quickly found their way into 2011's proposed bills. I expect the final report to be heavily influential on 2012's infosec and privacy debates.

Information security and data protection issues surrounding contracting for cloud services will begin the road to maturity in 2012 as the federal government continues pushing fed agency IT needs into the cloud. The result will help provide trickle down guidance on cloud contracting issues addressing audit assurances, cloud security and accreditation, e-discovery issues, security controls and allocation of liability and responsibility for data security, to name but a few.

Finally, 2012 will unfortunately see no end to advanced attacks resulting in data breaches, with attacks on and using mobile devices to ramp up significantly. In response the move to Big Data and data hoarding may reverse as companies in specific sectoral areas begin paring back on how much data they retain.

Follow Richard Santalesa on Twitter:
@RichNet

CONCERNS OVER BYOD AND COIT

InfoLawGroup Partner, David Navetta

Predicts a growing importance in 2012 "of key buzz words that implicate data security and privacy issues, such as are BYOD ("Bring Your Own Device") and COIT ("Consumerization of Information Technology"). Based on societal trends concerning portable computing devices, tablets and smart phones, and due to potential cost saving considerations, more companies are going to let their employees store and process information on their own personal computing devices. The security associated with those devices will be at issue, as will incident response considerations, and the privacy of the individuals who are using their personal devices for dual purposes."

Follow David Navetta on Twitter:
@DavidNavetta

→ SMB'S BECOME A TARGET FOR DATA BREACHES IN 2012
→ INCREASED CYBER ATTACKS
→ GROWTH IN WEBSITE ATTACKS
→ MOBILE THREATS
→ HACKTIVISTS TARGET THE CLOUD

Bruce Anderson, CEO, Cyber Investigation Services, says…

As we roll into the new year of 2012 I've had a chance to reflect on where the industry is headed and what trends are we going to see as it relates to Cyber Security and Data Breaches in 2012. According to the Verizon 2011 Data Breach Investigations reports, there were some very tell tale signs that gives us a heads up for what to expect in 2012 combined with the actual calls that we receive concerning cyber attacks as an agency.

1. Data Breaches are going to grow in 2012 and will be targeting companies with 11-100 employees due to their lack of sophistication and budget to hire full time security groups to protect their data. Targeted attacks will be on the rise.

2. The growth of the Bot-Nets like Spy Eye and Zeus that take advantage of zero day and undetectable malware will continue to grow as the development and ease of purchase by "script kiddies" will continue to proliferate.

3. We will see a growth in website attacks such as Web Hijacking, DDOS and Data Intrusions for the purpose of paid extortion of individuals and companies as well as competitors seeking to gain unfair advantage.

4. While federal agencies are gearing up to combat terrorist threats, threats to our infrastructure and banking systems, with increased tools to combat Cyber Attacks, the growth of cyber fraud and civil torts will grow due to the lack of training and manpower of local police agencies and District Attorneys to address the growing use of the internet and attacks associated with it. These attacks will be structured to stay under the radar of the Feds, while at the same time take advantage of

(continued) Bruce Anderson, CEO, Cyber Investigation Services

jurisdictional complexities, finances to fight the attack, and lack of resources by local and state governments.

5. While the trends point toward more privacy controls for individuals the actuality will be that technology, mobile computing and the growth of IPV6 will actually make the invasion of privacy easier for those that seek to invade others privacy. In short it will be very difficult to legislate privacy policy that will really work.

6. While there is a big move towards towards cloud computing by both large and small organizations, Hacktivist groups like Anonymous will make headway in penetrating large companies, and government agencies through the cloud which will cause significant alarm in the Security world on how to protect their clients and keep their confidence in the growing industry of cloud computing.

CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Anthony M. Freed, Managing Editor at Infosec Island predicts…

"Industrial control systems (ICS) like supervisory control and data acquisition (SCADA) networks are ill prepared to cope with current and emerging threats. ICS-SCADA systems provide operations control for critical infrastructure and production networks including manufacturing facilities, oil and gas refineries, the public water supply, and in electricity production and nuclear power plants, to name just a few. I believe we will see a lot of activity in 2012 from those who seek to disrupt these operations - be they hacktivists, nation-state aligned hackers, or criminal syndicates. On a positive note, as general awareness of the numerous vulnerabilities grows, I think we will see a tremendous effort to mitigate those threats by industry stakeholders, the government, and the security field. Hopefully adequate remediation efforts will prevail over available exploits prior to an event of any magnitude."

Follow Anthony M. Freed on Twitter:
@anthonymfreed

FTC USING EXISTING POWERS TO REGULATE COMMERCIAL ENTERPRISES

Shaun Dakin, Managing Director, Webbmedia Group
Founder @PrivacyCamp
Founder #PrivChat, a weekly Twitter conversation on privacy issues.

2011 was the year of multiple privacy related bills in the US Congress (last count 19 bills in the house and the senate).

These bills did not get passed. Mostly, the hearings associated with the bills made for good political theater as Members of Congress called industry representatives from Facebook, Google and Apple to testify in front of the cameras.

Meanwhile the FTC was using it's limited authority to make settlements with Google (for Google Buzz) and Facebook for around privacy violations.

As stated by the FTC: "*The social networking service Facebook has agreed to settle Federal Trade Commission charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.*"

So, 2011 was the year of the FTC flexing its regulatory authority and thereby setting the standards around data privacy for all businesses to adhere to without a single new bill passing into law.

2012 should bring more of the same from the FTC.

Follow Shaun Dakin on Twitter:
@ShaunDakin
@PrivacyCamp

CHANGES IN AMERICA INVENTS ACT WILL DRIVE INTELLECTUAL PROPERTY OWNERS TO EXPLORE SPECIALIZED IP INSURANCE POLICIES TO FUND IP LIGITATION

Robert Fletcher, founder and CEO of Intellectual Property Insurance Services Corporation (IPISC) bfletcher@patentinsurance.comm

Due in part to the America Invents Act of 2011, experts predict that, at least in the short term, patent litigation may actually increase in frequency and duration instead of decreasing, which will result from parties racing to the courthouse to beat some of the provisions that do not take effect immediately, and to avoid uncertainly as to how the new laws will be applied and interpreted.

Legal costs are also expected to increase as even more specialized expertise will be required to navigate the new changes to the patent law, which are intended to strengthen US issued patents. Companies must have a plan in place to enforce their rights to meet the anticipated rise in litigation. They must either have a well-funded war chest in place, or have adequately transferred their intellectual property risk via specialized IP insurance policies to fund IP litigation.

As a result of patent reform, patents are expected to become stronger and more valuable, making companies more likely to enforce their patent rights. Frequently, patent enforcement activities increase with a slow economy because patent owners seek to protect the exclusivity of their patented markets while entrepreneurs are will to copy products that are selling well.

While the America Invents Act may limit the litigious disposition of some non-practicing entities, others will continue will to almost arbitrarily accuse companies of infringing activity. Due to all of the above uncertainties, companies are realizing now more than ever that it is critical to have protection for their intellectual property assets in place through specialized IP insurance products.

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.

We help many different types of businesses and health care organizations create a Data Breach response plan and help protect their Cyber Risks and (IP) Intellectual Property. Whether you are a Hospital concerned about creating a data breach incident response plan, a Cloud provider concerned about liability, an App Developer worried about a software patent lawsuit or an Ecommerce website concerned about PCI-DSS, we have an insurance market for your risk.

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.

CYBER DATA RISK MANAGERS LLC
4400 Route Highway 9 South, Suite 1000
Freehold, New Jersey 07728
US toll free: 1 +855.CUT.RISK
Fax: 1 +732.709.1684
www.DataPrivacyInsurance.com
Follow us on Twitter: @DataPrivacyRisk