INSURANCE INFORMATION INSTITUTE

SOCIAL MEDIA, LIABILITY AND INSURANCE

DECEMBER 2011

Robert P. Hartwig, Ph.D., CPCU
President & Economist
(212) 346-5520
bobh@iii.org

Claire Wilkinson
(917) 459-6497
clairew@iii.org

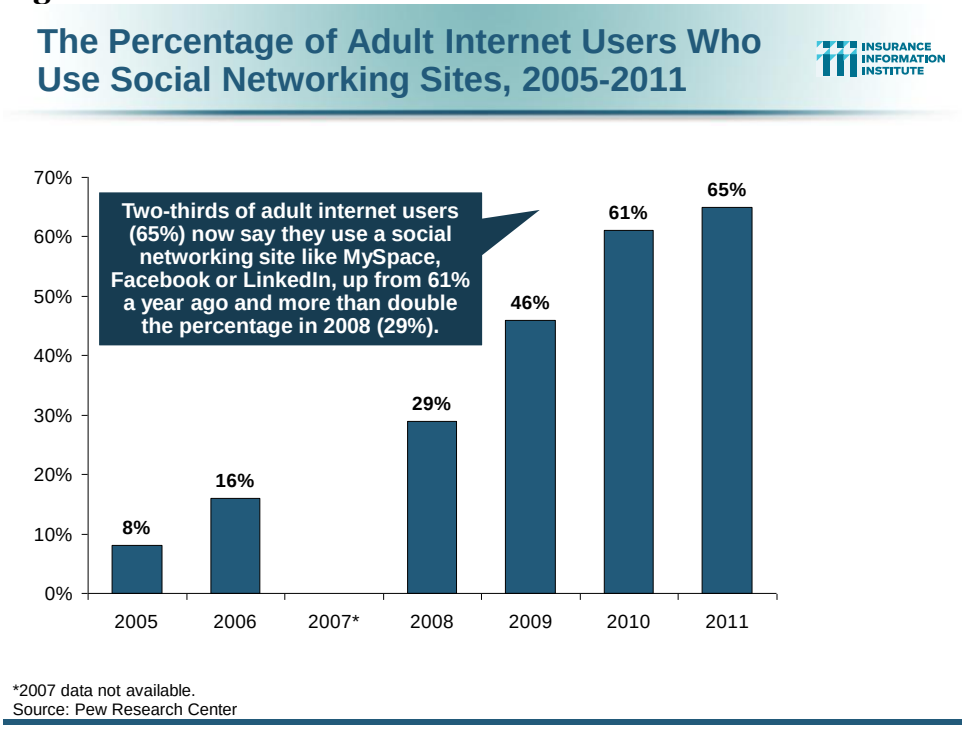
Social Media: An Evolution

INTRODUCTION

Hundreds of millions of people interact on social networks like Facebook, Twitter, YouTube, MySpace and LinkedIn every day. In fact some 65 percent of adult Internet users now say they use a social networking site, according to a recent report from the Pew Research Center.[1]

The Pew study found that in the last six years the number of Americans using social networking sites has surged. In 2005, just 8 percent of adult Internet users reported using social networking sites (Fig.1).

Fig.1

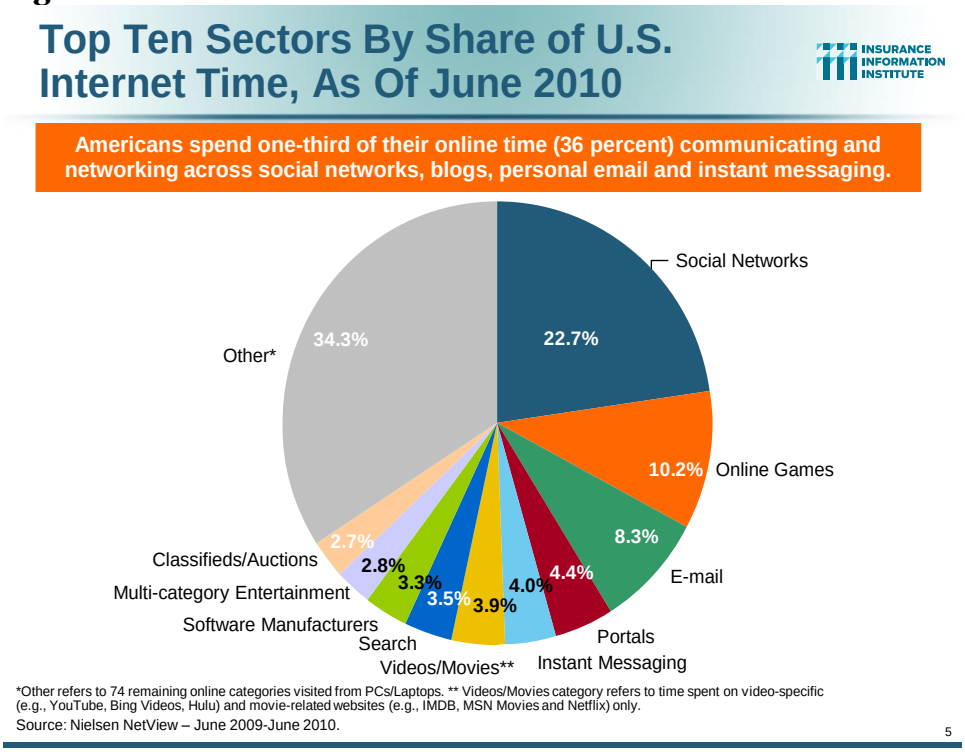


Earlier research by The Nielsen Company also found that Americans spend nearly a quarter (22.7 percent) of their time online on social networking sites and blogs, up from 15.8 percent the previous year (a 43 percent increase) (Fig. 2).[2]

[1] *65% of online adults use social networking sites*, Pew Research Center, August 2011, http://pewinternet.org/Reports/2011/Social-Networking-Sites.aspx

[2] Nielsen NetView, June 2009-2010, http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/

Fig.2



Like any other new technology, social media brings enormous opportunities and benefits. The ability to communicate and interact instantaneously on a global scale 24/7 enables businesses to reach their customers directly and individuals to voice opinions on any topic they see fit.

Yet as the opportunity to tweet, message, share and "like" grows, so do the risks. For example, in recent months social media has been used as a key form of communication in the Occupy Wall Street protests, as an enabler of the grassroots uprisings in the Middle East, and as a tool used by rioters to incite and coordinate civil disorder in the United Kingdom. Two U.K. men were actually jailed for four years each for inciting disorder via social networking sites.

Just one disparaging tweet on a company's product or service has the potential to trigger a viral reputation meltdown if a business does not provide an immediate and effective response. Social networking sites raise customer awareness on a global scale, in some cases even helping people to make a claim for a faulty product or for a personal injury.

A recent Consumer Reports survey also found that social media use by households is exposing them to a range of risks, including virus thefts and identity theft. [3]

[3] 2011 State of the Net Survey, Consumer Reports Magazine, June 2011, http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/online-exposure/index.htm

Meanwhile, there are growing concerns about social media and consumer privacy. U.S. representatives Edward Markey and Joe Barton, co-chairs of the Congressional Bi-Partisan Privacy Caucus, recently wrote to the Federal Trade Commission (FTC) asking it to look into the way Facebook tracks user activity.

And in a sign of the growing potential liability faced by social media and online companies, Facebook Inc. has reached a settlement with the Federal Trade Commission (FTC) over its privacy policies.[4] Among other things the settlement will require Facebook to obtain consent from users each time it retroactively changes its privacy policy and to establish and maintain a comprehensive privacy program designed to address privacy risks associated with its products and services.

Key social media liability and risk-related news stories from 2011 include New York State Senator Anthony Weiner's resignation from Congress due to a sexting scandal that began when he accidentally posted a link to an inappropriate picture of himself on his public Twitter account, and singer Courtney Love's settlement of a defamation lawsuit for $430,000 after being sued by her former designer for allegedly libelous statements posted by Love on her Twitter account. Social media related risks such as cyber-bullying and textual harassment are also leading to growing exposures for school districts and educational institutions.

There are many more examples like these, but what is clear is that the growing use of social media in everyday life is giving rise to a range of evolving liabilities. Industry experts say this is creating a whole new world of privacy, security, intellectual property, employment practices and other risks for businesses and individuals.[5]

The proliferation of social media use comes amid growing concerns over cyber security. Businesses that store confidential customer and client information online are exposed to increasing liabilities and costs as a result of cyber attacks and data breaches. Indeed, total data breach costs have increased every year since 2006, according to the Ponemon Institute (see later section on cyber security).

Some 340 organizations across business, financial, educational, government and healthcare sectors, have publicly disclosed data breaches in 2011 as of November 1, according to the Identity Theft Resource Center.[6] This compares to 662 publicly disclosed data breaches during 2010.

A massive data breach at Sony Corp's online game networks in April 2011 resulted in the theft of more than 100 million online accounts, for example. Just months

[4] *What the Facebook/FTC Settlement Means for Users*, by Larry Magid, Huffington Post, December 6, 2011.
[5] *Social Media: The Business Benefits May be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?*, ACE and InfoLawGroup, April 2011.
[6] Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202011.pdf

later in October 2011 Sony's Playstation Network and other online entertainment services were hit in a second attack that compromised 93,000 user accounts.

Coming in the wake of the 2010 Wikileaks breaches of classified data, these high profile data breach incidents have served to increase both public and government scrutiny of cyber security practices.

A hacker group known as Anonymous has also drawn the attention of the FBI and other federal investigators after much-hyped cyber threats, announced in video messages on YouTube or via Twitter, some of which appear to have crashed the websites of governments and financial institutions.

The Securities and Exchange Commission (SEC) recently issued guidance urging publicly traded companies to disclose significant instances of cyber risks and events.[7] Description of relevant insurance coverage was included in the SEC's list of appropriate disclosures.

Meanwhile, a number of federal legislative/regulatory proposals on cybersecurity, including data breach notification, are under consideration by Congress. At the state level, some 46 states also have breach notification laws in effect. A summary of the various bills is included in **Appendix 1**.

SOCIAL MEDIA LITIGATION

Given the proliferation of social media and its growing use in everyday life, it's not surprising that litigation has started to emerge. Lawsuits range from the absurd—such as a Michigan woman suing a man for more than $8,000 in damages after a romance sparked on Facebook failed—to the serious.

Two highly-publicized cases, widely regarded as potential test cases in this area, have involved the singer Courtney Love. In May 2011, Love was sued for alleged defamation on Twitter by former lawyers who had represented her in 2008 in an effort to recover money allegedly stolen from the estate of her late husband, Kurt Cobain. [8] In the lawsuit San Diego-based law firm, Gordon & Holmes, alleges Love made libelous statements about them on Twitter.

Just two months earlier in March 2011, Love agreed to pay $430,000 plus interest, to settle a landmark Twitter defamation lawsuit brought in March 2009 by her former designer over comments Love made on her Twitter and MySpace accounts. Even though the case did not go to trial, several reports cite legal experts saying that it highlights the need for celebrities and average people to watch what they say online.[9]

[7] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[8] *Courtney Love Sued Again For Defamation On Twitter,* by Matthew Belloni, Hollywood Reporter, May 26, 2011.
[9] *Courtney Love Settles $430,000 Twitter Defamation Lawsuit,* by Anthony McCartney, Huffington Post, March 4, 2011.

Other social media cases that have attracted significant attention have been in the employment arena. According to a recent U.S. Chamber of Commerce study, the National Labor Relations Board (NLRB) has received an increasing number of charges involving employee use of social media and employers' social media policies in the past year.[10] The issues most commonly raised in the cases before the NLRB allege that an employer has overbroad policies restricting employee use of social media or that an employer unlawfully discharged or disciplined one or more employees over contents of social media posts.

For example, in September 2011 a National Labor Relations Board (NLRB) Administrative Law Judge found that the Buffalo nonprofit organization, Hispanics United of Buffalo, had unlawfully discharged five employees after they posted comments on Facebook about working conditions, including work load and staffing issues. The nonprofit was ordered to reinstate the five employees with back pay. The judge found that the employees' Facebook discussion was protected concerted activity under the National Labor Relations Act because it involved a conversation among coworkers about their terms and conditions of employment. This was the first social media case involving a non-union employer.

An earlier landmark NLRB case involving a Connecticut ambulance company was settled in February 2011. In this case NLRB had issued a complaint against American Medical Response of Connecticut, Inc. (AMR) in October 2010, after it terminated an employee who had criticized her supervisor on Facebook. The Complaint alleged that AMR's social media policy itself, and not just the employee's termination, violated the National Labor Relations Act (NLRA). The settlement agreement called for AMR to make changes to its social media policy. A separate, private settlement reached between AMR and the employee resolved the allegations surrounding her firing.

Meanwhile, litigation surrounding data and privacy protection continues to evolve amid a growing number of high profile data breaches. In the 2011 litigation trends survey by Fulbright & Jaworski, corporate counsel, polled in the U.S. and U.K., reported that privacy and data protection issues arose most frequently in the context of collecting data from company equipment used by employees (57 percent of all respondents encountered an issue) and employees' personal equipment (50 percent of all respondents encountered an issue).[11]

The Fulbright survey also asked questions on how social media arises in the context of litigation. It found that nearly one-fifth of all respondents reported that in the previous year their companies had to preserve or collect data from an employee's personal social media account.

[10] *A Survey of Social Media Issues Before the NLRB*, U.S. Chamber of Commerce, August 5, 2011.
[11] *Fulbright's 8th Annual Litigation Trends Survey Report*, Fulbright & Jaworski, October 2011.

Furthermore, some 13 percent of all respondents have had to produce, as part of discovery, electronic information stored on a social media site in the past 12 months.

LEGAL LIABILITY

Given the sheer volume of individuals and businesses that post content on or contribute to online networks and social media sites there are numerous potential avenues of legal liability that may be pursued. Many of the areas of potential legal liability are similar to those faced by a traditional publisher.

Some of the key areas where liability could arise for companies include:[12]

Advertising Liability: Businesses have a legal responsibility to ensure that their advertising is truthful and not deceptive. The Federal Trade Communication Act and various state laws that prohibit false or deceptive advertising apply to online ads too. The FTC has also revised its endorsement guidelines to include advertising via social media, requiring bloggers and advertisers to disclose any "material connections" with each other. So if an advertiser pays a blogger or gives a blogger something of value to mention a product, that relationship must be disclosed.

Cyberstalking: Many states have enacted cyberstalking or cyberharassment laws. Some states include language addressing electronic communications in general harassment statutes, while others have created stand-alone cyberharassment statutes. Growing concerns about protecting children from online bullying or harassment have also led states to enact cyberbullying laws. Statutes and laws may cover a range of activities such as: threatening physical violence; hacking into computers and sending viruses; transmitting obscene or intentionally annoying emails; the willful and repeated use of cellphones, computers and other electronic communication devices to harass and threaten others.

Defamation: Defamation is the publication of false and defamatory statements that harm or injure the reputation of another person or company. Trade libel under common law or statute also applies to false statements that disparage another's goods or services. Truth is a complete defense in a defamation case. Statements may be protected if they constitute only opinion and are not capable of being proven true or false.

Employers' Liability: Employers increasingly are using social media to investigate potential and existing employees. For example, a 2010 Career Builder survey found that one-quarter (21 percent) of companies use social media sites to recruit and research potential employees. A company that fires an employee based

[12] *Social Media: The Business Benefits May be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?*, ACE and InfoLawGroup, April 2011.
More Media, More Opportunity, More Risk, by Damon Dunn, Risk Management Magazine, October 2010.
Minimizing the Legal Risks of Using Online Social Networks, by Lawrence Savell, as appeared in Law.com June 28, 2010.

on their social media interactions with other employees may find themselves in violation of the National Labor Relations Act (NRLA). The language of a company's social media policy could be construed as overly broad and in violation of the NRLA. Another concern raised in the employment arena is improper solicitation. This occurs when an employee changes jobs and uses social media to contact former clients from their previous position. In some industries, non-solicitation agreements may be in place, but how these apply to social media may not be clear. This is an area where employers are likely to craft specific rules to protect their interests.[13]

Intellectual Property: Copyrighted video, audio, images and other works created by a third party should not be posted or reposted without permission. Employees who post content created by others should include proper attribution and limit the quotations to "fair uses" of copyrighted content.

Privacy Liability: Companies may have an obligation to protect the privacy of members of the public who join their social networking pages or provide personal information through social media sites. Privacy protections that may apply include: use (appropriation) of a person's name, portrait or picture for advertising or commercial purposes without prior explicit consent; public disclosure of private or embarrassing facts about a person; statements portraying someone in a false light (similar to libel). Information may also be protected from disclosure by federal and state statutes, such as the Health Insurance Portability and Accountability Act (HIPAA) that provides for the privacy of medical records.

Security Breach Liability: An organization may be found liable if a breach arising from social media and online activities compromises the security of customer personal information or data. A company may also be found negligent if a breach resulted from a systems failure, for example. Increased regulation at both the Federal and state level related to information security and breach notification is expanding the legal avenues that may be pursued. Many states have enacted laws requiring companies to notify consumers of breaches of personal data. Federal laws, such as the HIPAA and the Gramm Leach Bliley Act have requirements to safeguard the privacy of personal information.

Trade Secrets: A company may face liability if its employees post competitors' trade secrets and confidential information online. Businesses can also forfeit protection of their own confidential information if employees allow it to leak online.

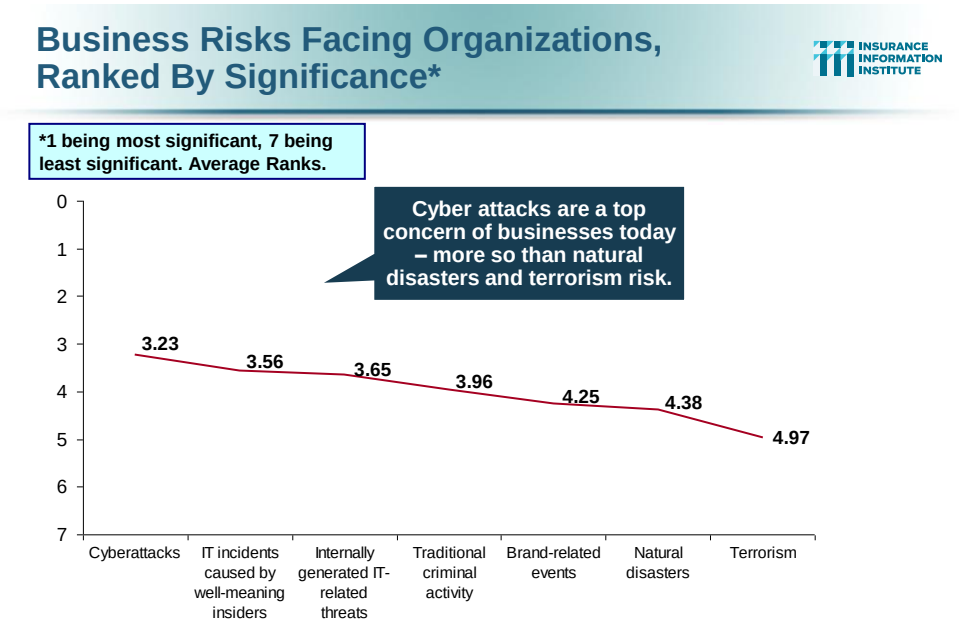
[13] *Investing in Funds: A Monthly Analysis*, The Wall Street Journal, November 7, 2011.

CYBER SECURITY

Cyber security and losses from cybercrimes are a growing concern among businesses today. In its Global Risks Report 2011, the World Economic Forum (WEF) identified cyber security as one of the top five risks to watch, up there with demographic challenges and weapons of mass destruction, among others. The complexity of cyber security issues, ranging from cyber theft to all-out cyber warfare, is still not well understood and its risks could be underestimated, the WEF said.

While companies are focused on a variety of business risks, including natural disasters and terrorism, their top concern appears to be cyber attacks, according to a recent survey conducted for Symantec by Applied Research (Fig.3).

Fig. 3

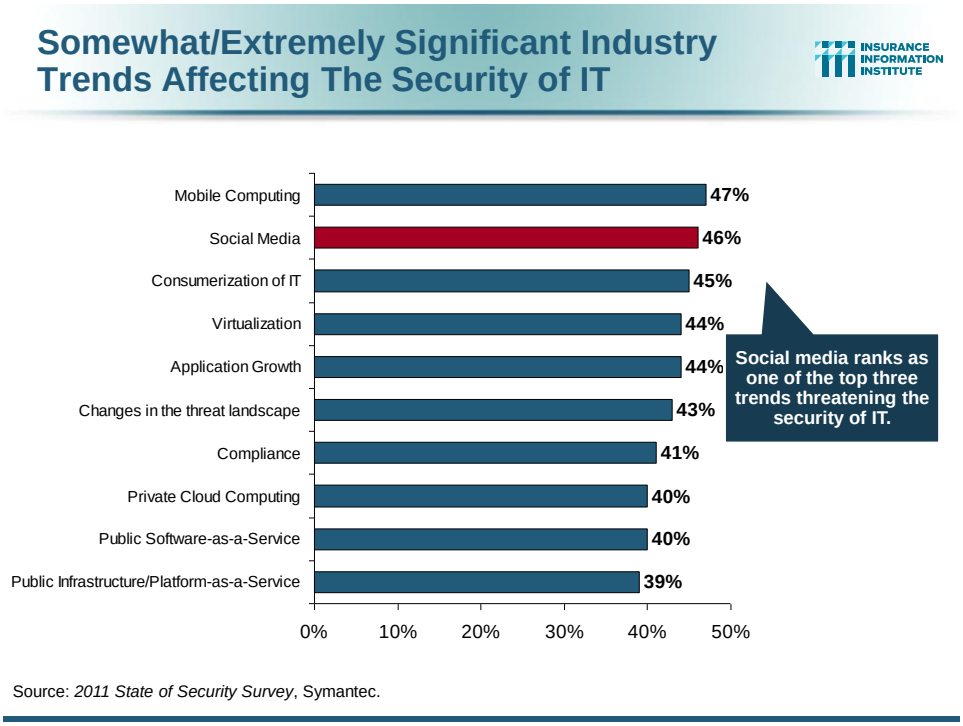


Source: *2011 State of Security Survey*, Symantec.

The importance of managing cyber threats to companies also appears to be increasing, Symantec found. Some 41 percent of respondents say cyber security is more important today than it was just a year ago, compared to just 15 percent who believe the importance of cyber security is somewhat or significantly decreasing.

As corporate cyber security concerns increase, the survey also found that social media was one of the top trends threatening cyber security, cited by 46 percent of respondents, and second only to mobile computing (47 percent) (Fig. 4).

Fig.4

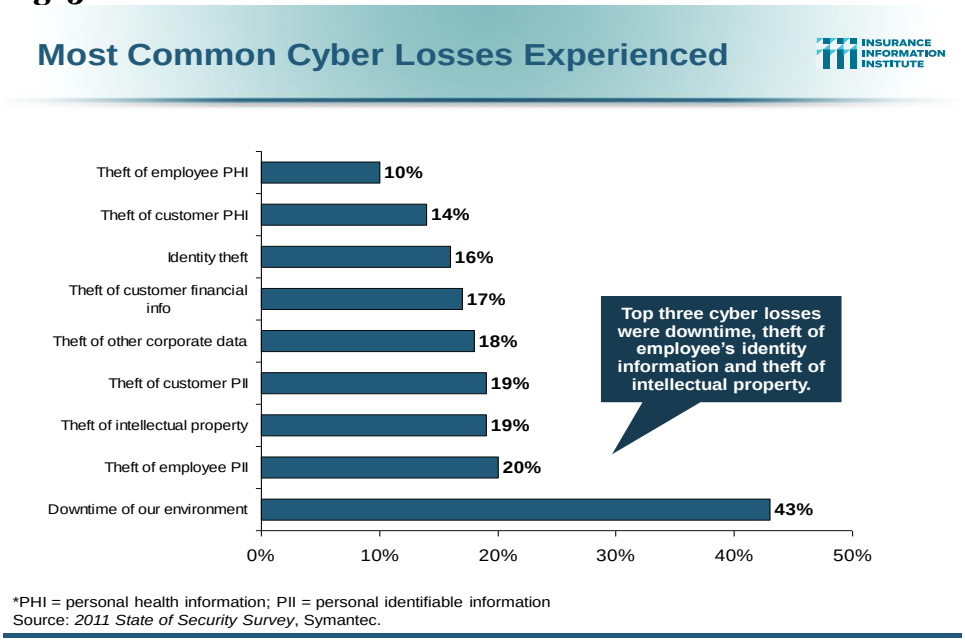


Source: *2011 State of Security Survey*, Symantec.

Organizations report that the threats they are facing are also evolving. Hackers are still their top concern, cited by 49 percent, followed by well-meaning insiders (46 percent).

Ninety-two percent of companies saw losses from cyber attacks in the last year. The top three reported losses were downtime, theft of employee's identity information and theft of intellectual property (Fig. 5).

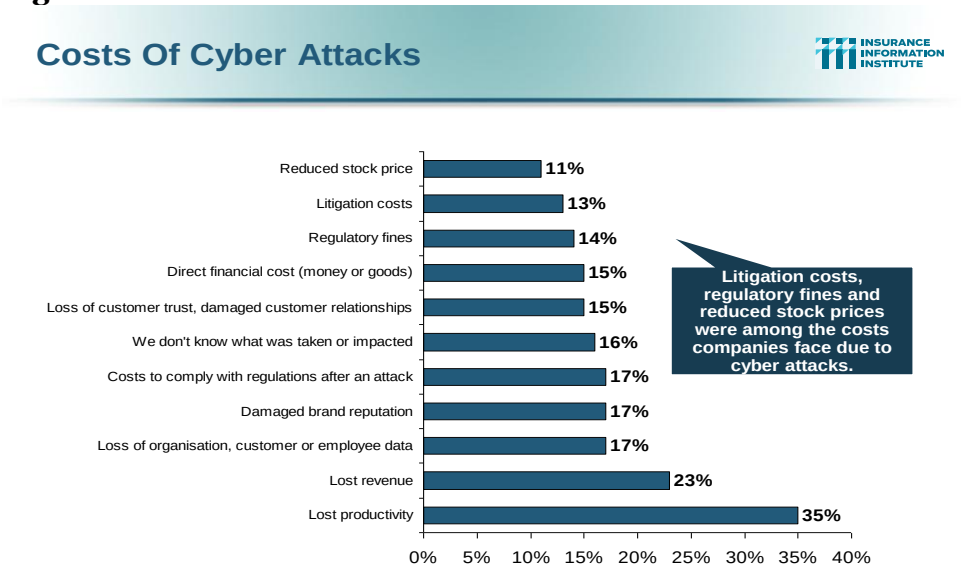
Fig. 5



*PHI = personal health information; PII = personal identifiable information
Source: *2011 State of Security Survey*, Symantec.

These losses translated to monetary costs 84 percent of the time, according to Symantec. The top costs were: lost productivity; lost revenue; loss of organization, customer or employee data; and damage to a company's brand reputation. Litigation costs, regulatory fines and reduced stock price were also among the costs companies face (Fig. 6).

Fig. 6



Source: *2011 State of Security Survey*, Symantec.

Symantec noted that 20 percent of businesses lost at least $195,000 as a result of cyber attacks. Among larger companies, 20 percent incurred at least $271,000 in expenses from attacks within the last year.

DATA BREACHES: RISING COSTS AND LIABILITY EXPOSURE

Businesses that store confidential customer and client information online are exposed to increasing liabilities and costs as a result of data breaches.

Some 340 organizations across business, financial, educational, government and healthcare sectors, have publicly disclosed data breaches in 2011 as of November 1, according to the Identity Theft Resource Center.[14] This compares to 662 publicly disclosed data breaches during 2010.

Recent high profile data breach incidents include a massive data breach at marketing services firm Epsilon in March 2011 that involved a long list of companies from retailers to hotel chains to financial firms. And another massive data breach at Sony Corp's online game networks in April 2011 resulted in the theft of more than 100 million online accounts (Fig. 7).

Fig. 7

High Profile Data Breaches, 2011

INSURANCE INFORMATION INSTITUTE

As of November 1, 2011, an estimated 340 data breaches have exposed some 22.3 million records, according to the Identity Theft Resource Center.

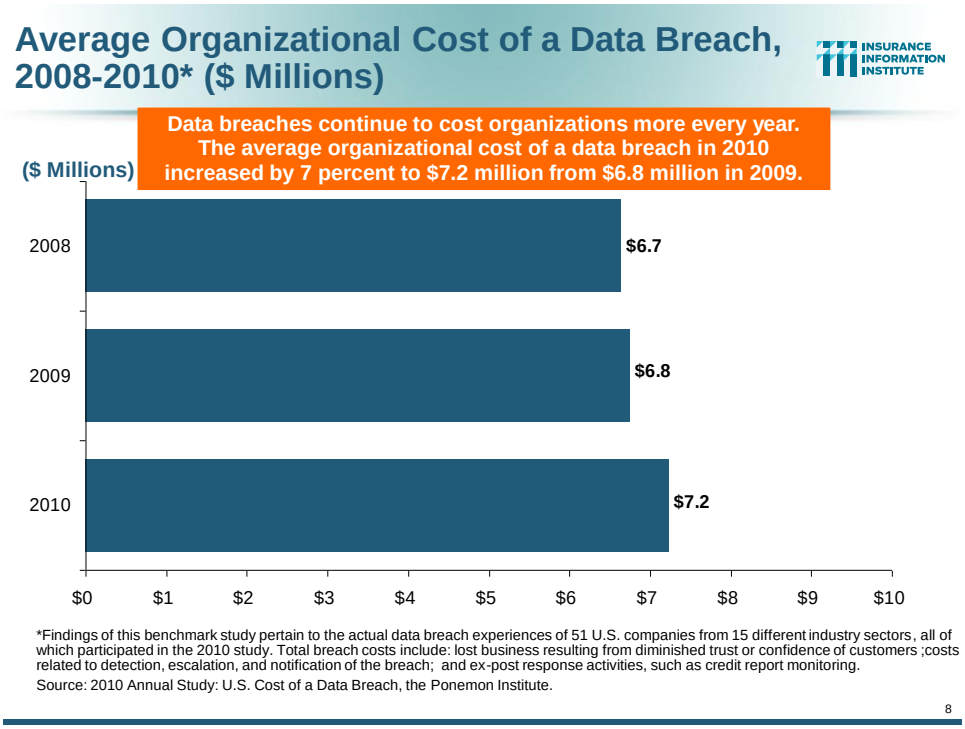
Date	Company	Description of Breach
Oct 2011	Sony Corp	Hacker attack at Sony's Playstation Network and other online entertainment services compromises 93,000 user accounts.
Sept 2011	TRICARE	Military health plan TRICARE discloses personal data of 4.9 million beneficiaries could be at risk after data breach reported by contractor Science Applications International Corp (SAIC).
July 2011	Pentagon	The Pentagon reveals that in March 2011, some 24,000 files were stolen from a defense industry computer network.
June 2011	Citigroup	Banking and insurance giant Citigroup announces that hackers breached its computer systems, taking personal identity information of some 200,000 clients.
May 2011	Lockheed Martin	Network intrusion at U.S. defense contractor Lockheed Martin linked to hacker attack on RSA's SecurID authentication tokens.
April 2011	Sony Corp	Massive data breach at Sony Corp's online game networks results in the theft of more than 100 million online accounts.
March 2011	Epsilon	At least 26 firms, including BestBuy, Capitol One, Citi, JPMorgan Chase, TiVo and Walgreens have their customer email lists stolen after data breach at marketing services firm Epsilon.
Feb 2011	Nasdaq	Nasdaq confirms that hackers breached its computer network, targeting an application called Directors Desk, an application that stores financial records and reports for Fortune 500 and corporate board members.

Sources: Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202011.pdf; Insurance Information Institute (I.I.I.) research.

[14] Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202011.pdf

A benchmark study of 51 U.S. companies by the Ponemon Institute found that the average cost of a data breach increased to $7.2 million in 2010, up 7 percent from $6.8 million in 2009 (Fig. 8).[15] The average breach cost companies $214 per compromised record up from $204 in 2009, it found.

Fig. 8

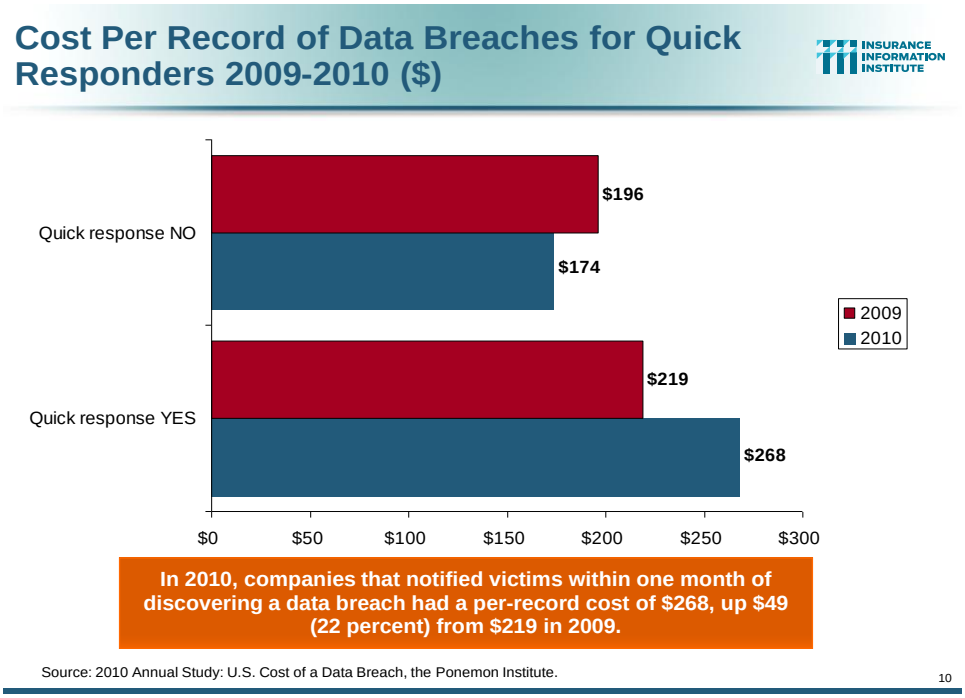


For the first time, malicious or criminal attacks were the most expensive cause of data breaches and not the least common one. Nearly one-third (31 percent) of all cases in the study involved a malicious or criminal attack. Breach costs for malicious attacks skyrocketed with the 2010 cost per compromised record of a data breach involving a malicious or criminal act averaging $318, up $103 (48 percent) from 2009 and the highest of any data breach cause.

[15] *2010 Annual Study: U.S. Cost of a Data Breach*, research by the Ponemon Institute, sponsored by Symantec, March 2011, http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

The Ponemon study also found that the need for organizations to respond rapidly to data breaches drove the associated costs higher (Fig. 9).

Fig. 9



In 2010, companies that notified victims within one month of discovering the breach had a per-record cost of $268, up $49 (22 percent) from $219 in 2009. Companies that took longer to respond paid $174 per record, down $22 (11 percent) from 2009.

This means that rapid response to data breaches is costing companies 54 percent more per record, on average, than companies that moved more slowly.

The notable increase in companies responding quickly to breaches, despite the additional cost, may reflect pressure they feel to comply with commercial regulations and state and federal data protection laws, the study said.

It also noted that the federal government and attorneys general in some states, such as Massachusetts, can sue companies for negligence if the government officials believe the companies are not responding to a data breach sufficiently fast. More companies could be spending more than necessary to respond quickly to breaches to avoid possible regulatory scrutiny and penalties, it added.

As new technologies continue to evolve, companies are exposed potentially to even greater risks from data security breaches. For example, security concerns surround

the adoption of cloud computing—the use of a network of remote servers over the Internet to store, manage and process data, rather than a local server—by both companies and government agencies.

Nearly 25 percent of global business leaders believe that the use of cloud technologies has increased the information security vulnerability of their company, according to a recent survey by PricewaterhouseCoopers.[16] Furthermore, in the 2011 litigation trends survey by Fulbright & Jaworski, more than one-quarter of respondents who use cloud computing report they have encountered security breaches.

SOCIAL MEDIA, CYBER SECURITY LIABILITY AND INSURANCE

While traditional insurance policies typically have not handled these emerging risks, in recent years limited coverage under traditional policies has become available.

Traditional business insurance policies that policyholders and their lawyers may look to for coverage in the event of a data breach or other cyber-related attack include: property insurance (including business interruption coverage); liability insurance (including E&O, D&O, general liability and umbrella insurance); crime insurance policies (including financial institution bonds, computer crime policies and fidelity insurance); and businessowners policy (BOP) packages.[17]

However, as reliance on traditional insurance policies is not enough, specialist social media and cyber insurance policies have been developed by insurers to help businesses and individuals protect themselves from an ever-evolving range of risks.

A recent Advisen survey sponsored by Zurich, found that while a growing number of risk professionals acknowledge information security and other cyber risks as serious concerns, only about one-third of organizations (35.1 percent) currently purchase insurance as part of their cyber risk management strategy.[18]

Some key reasons survey participants gave for not purchasing cyber liability insurance included:

- Investment in prevention rather than insurance
- Limited markets
- Broker disconnects
- Lack of coverage clarity
- Lack of information to make informed decisions

[16] *2012 Global State of Information Security Survey*, PricewaterhouseCoopers, November 2011.
[17] *Data Security Insurance for Cyber-Related Losses*, by Joshua Gold, Policyholder Advisor, May/June 2011, Anderson Kill + Olick, P.C.
[18] *A New Era In Information Security and Cyber Liability Risk Management,* by Advisen, sponsored by Zurich, October 2011.

- Too expensive
- Application process is difficult
- Deductibles are too high
- Difficult to quantify
- Policy coverage is too limited

Advisen did report that interest in the coverage appears to be growing, as an increasing number of companies have purchased protection in recent years or are considering buying coverage in the near future.

Guidance issued by the Securities and Exchange Commission (SEC) in October 2011 urging publicly traded companies to disclose significant cyber risks and events is likely to increase the purchase of cyber insurance by public companies in the months ahead.

Specialized cyber risk coverage is available primarily as a stand-alone policy. Each policy is tailored to the specific needs of a company, depending on the technology being used and the level of risk involved. Both first- and third-party coverages are available.

Types of cyber risk coverage include:

Loss/Corruption of Data: Covers damage to, or destruction of, valuable information assets as a result of viruses, malicious code and Trojan horses.

Business Interruption: Covers loss of business income as a result of an attack on a company's network that limits the ability to conduct business, such as a denial-of-service computer attack. Coverage also includes extra expenses, forensic expenses and dependent business interruption.

Liability: Covers defense costs, settlements, judgments and, sometimes, punitive damages incurred by a company as a result of:

- Breach of privacy due to theft of data (such as credit cards, financial or health related data);
- Transmission of a computer virus or other liabilities resulting from a computer attack that causes financial loss to third parties;
- Failure of security that causes network systems to be unavailable to third parties; Rendering of Internet Professional Services;
- Allegations of copyright or trademark infringement, libel, slander, defamation or other "media" activities on the company's website, such as postings by visitors on bulletin boards and in chat rooms. This also covers liabilities associated with banner ads for other businesses located on the site.

Cyber Extortion: Covers the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.

Crisis Management: Covers the costs to retain public relations assistance or advertising to rebuild a company's reputation after an incident. Coverage is also available for the cost of notifying consumers of a release of private information, as well the cost of providing credit-monitoring or other remediation services in the event of a covered incident.

Criminal Rewards: Covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of a cyber criminal who has attacked a company's computer systems.

Data Breach: Covers the expenses and legal liability resulting from a data breach. Policies may also provide access to services helping businessowners to comply with regulatory requirements and to address customer concerns.

Identity Theft: Provides access to an identity theft call center in the event of stolen customer or employee personal information.

Social Media/Networking: Insurers are looking to develop products that cover a company's social networking activities under one policy. Some cyber policies now provide coverage for certain social media liability exposures such as online defamation, advertising, libel and slander.

Depending on the individual policy, specialized cyber risk coverage can apply to both internally and externally launched cyber attacks, as well as to viruses that are specifically targeted against the insured or widely distributed across the Internet. Premiums can range from a few thousand dollars for base coverage for small businesses (less than $10 million in revenue) to several hundred thousand dollars for major corporations desiring comprehensive coverage.

As part of the application process, some insurers offer an online and/or on-site security assessment free of charge regardless of whether the applicant purchases the coverage. This is helpful to the underwriting process and also provides extremely valuable analysis and information to the company's chief technology officer, risk manager and other senior executives.

Individuals are also seeking to better protect themselves from the risks created by their participation in social media. While traditional homeowners insurance policies include liability protection that covers the insured against lawsuits for bodily injury or property damage, coverage may be limited and individual policies may differ by company and by state. Case law in this area is also evolving and still uncertain. Umbrella or excess liability policies provide broader protection, including claims against the insured for libel and slander, as well as higher liability

limits. Specialized insurance products that protect an individual from social media related risks are under development.

RISK MANAGEMENT

When it comes to social media and cyber risks in general, insurance is only one tool in the risk management box.

Preparing a disaster plan ahead of time that can be activated in the event of a cyber attack or data breach, having a sound social media policy in place and training employees are just some of the other steps companies can take to help mitigate and reduce the risks.

In a recent poll by Advisen, sponsored by Zurich, some 68.6 percent of total respondents said that they have a disaster response plan in place, while only 16.5 percent said they do not and 14.7 percent did not know. The larger companies (revenue greater than $1 billion) represented a bigger portion of the total with 79 percent having a disaster response plan, compared to only 55 percent of companies with revenue under $1 billion.[19]

The Advisen survey also reported that of the companies surveyed, 63.6 percent have social media policies in place. The larger companies represented a bigger portion of companies who have social media policies in place, with 71 percent compared to 54 percent of the smaller companies.

An October 2011 report from law firm DLA Piper recently noted that while social media is being embraced in the corporate world, the pace at which it is developing is such that organizations' policies and procedures are struggling to keep up.[20]

DLA Piper found that many employers actively encourage the use of social media for work related activities (65 percent). However, 21 percent of employers have taken disciplinary proceedings because of information an employee displayed on a social media site about another individual, and 31 percent because of information posted about their organization.

Despite this, only a small proportion (25 percent) of businesses had a stand-alone, dedicated social media policy, and less than half (43 percent) had a social media policy which existed alongside another, such as an IT or HR policy, the report found.

[19] *A New Era In Information Security and Cyber Liability Risk Management,* by Advisen, sponsored by Zurich, October 2011.
[20] *Knowing Your Tweet From Your Trend: Keeping Pace With Social Media In The Workplace,* Shifting Landscapes Report 4, by DLA Piper, October 2011.

DLA Piper said the research highlights the need for a definitive social media policy which is regularly assessed and updated.

CONCLUSION

Like any other new technology, social media brings with it enormous opportunities and benefits. Yet as the opportunity to tweet, message, share and "like" grows, so do the risks. As businesses and individuals navigate this shifting online risk landscape, they face a range of evolving social media related liabilities including privacy, security, intellectual property and employment practices liability.

Meanwhile, amid a rising number of high profile data breaches, government is stepping up its scrutiny of cyber security. This is leading to increased calls for legislation and regulation, placing the burden on companies to demonstrate that the information provided by customers and clients is properly safeguarded online.

Despite the fact that cyber risks and cyber security are widely acknowledged to be a serious threat, a majority of companies today still do not purchase cyber liability insurance. However, research indicates that this is changing. Insurance has a key role to play as companies and individuals look to better manage and reduce their potential financial losses from social media and cyber risks in future.

Appendix 1

SUMMARY OF MAJOR CYBERSECURITY LEGISLATIVE PROPOSALS

Source: I.I.I. research and National Conference of State Legislatures (NCSL), as of September 2011.

Data Accountability and Trust Act (DATA) of 2011 (HR. 1841)
Summary: Would protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, and to provide for nationwide notice in the event of a security breach.

Data Breach Notification Act of 2011 (S. 1408)
Summary: Would require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information.

Data Security and Breach Notification Act of 2011 (S. 1207)
Summary: Would require reasonable security policies and procedures to protect data containing personal information, and provide for nationwide notice in the event of a security breach.

Personal Data Privacy and Security Act of 2011 (S. 1151)
Summary: A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

Personal Data Protection and Breach Accountability Act (S. 1535)
Summary: A bill to protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach. Would hold companies accountable for preventable security breaches, facilitate the sharing of post-breach technical information between companies, and enhance criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

State Legislative Developments: Since 2002, some 46 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, according to the National Conference of State Legislatures (NCSL).

In 2011, at least 14 states have introduced legislation expanding the scope of laws, setting additional requirements related to notification, or changing penalties for those responsible for breaches.