Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Insurance | the way we see it

Using Insurance to Mitigate Cybercrime Risk

Challenges and recommendations for insurers

People matter, results count.

Contents

1. Introduction

While technological advancements, evolving computer data systems, and internet access offer significant benefits to businesses and their customers, a major challenge that comes with the increased use of technology is an increase in the risk of cybercrime attack. Cybercrime has significant financial and non-financial implications for businesses.

To prevent cyber crime incidences, most companies employ cyber-security measures which include a combination of technology and security procedures. However, since cyber attackers are continuously discovering new ways to exploit vulnerabilities, cyber security alone cannot prevent all potential attacks.

This paper looks at how cybercrime insurance can protect companies from the costs of cybercrime. We explore the challenges for insurance companies offering cybercrime policies, analyze the required investments, and provide recommendations.

2. What is Cybercrime?

> “Cybercrime has become a silent global digital epidemic. The majority of internet users worldwide have fallen victim and they feel incredibly powerless against faceless cyber criminals.”
>
> *Cybercrime Report: The Human Impact*, Symantec, 2010

Cybercrime refers to any illegal activities using, or against, computer systems, computer networks, and the internet. Although cybercrime is a commonly used term today, there is no standard global definition and the definition varies based on the context. But while the term cybercrime describes a variety of attacks and activities, they can be broadly classified into three categories.

2.1. Category #1: Business Disruption and Misuse

- **Denial-of-Service (DOS) or Distributed Denial-of-Service (DDoS) Attack** refers to making a computer resource unavailable to its intended users or preventing it from functioning efficiently.
- **Malware or Malicious Software** refers to programs such as viruses and worms that try to exploit computer systems or networks leading to business disruption, leakage of sensitive data, or unauthorized access to system resources.
- **Software and Information Piracy** refers to theft or misuse of copyright material and software.
- **Industrial Espionage**[1] refers to corporate rivals illegally accessing confidential information to erode competitive advantage, gain financial information, or misuse trade secrets.
- **Cyber Extortion** refers to holding a company for ransom through denial of service, manipulating website links, or the threat of leaking customer or financial data.

2.2. Category #2: Online Scams

- **Phishing**[2] refers to disguising an electronic communication as coming from a trustworthy entity in an attempt to acquire sensitive data.
- **Spear Phishing**[3] refers to targeted campaign of highly personalized bogus e-mails, aimed at a specific individual or organization, that appear to come from a trusted source.
- **Pharming**[4] techniques involve redirecting website traffic from a legitimate website to a fraudulent website.
- **Spoofing** refers to fooling people into entering personal details into a counterfeit website.
- **Purchase Fraud** refers to selling products through online channels which are never shipped.

[1] “McAfee: Corporate Espionage Is the Currency of Cybercrime”, PC World Article, 2011, http://www.pcworld.com/businesscenter/article/223483/mcafee_corporate_espionage_is_the_currency_of_cybercrime.html
[2] “How to recognize phishing email messages, links, or phone calls”, Microsoft, http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx
[3] “Spear Phishing”, SearchSecurity.com, http://searchsecurity.techtarget.com/definition/spear-phishing
[4] The Cost of Cyber Crime, U.K. Cabinet Office and Detica, 2011

2.3. Category #3: Theft and Fraud

- **Identity Theft** refers to obtaining personal data from individuals—such as social security number, address, or bank account details—which can be misused to open new accounts or obtain services in the name of the victim.
- **Theft from Business** refers to stealing revenue directly from businesses using online channels; for example, obtaining access to a firm's accounts and transferring the money illegally.[4]
- **Intellectual Property (IP) Theft** involves stealing ideas, designs, specifications, trade secrets, or process methodologies, which may erode competitive advantage in terms of operations and technology.
- **Customer Data Theft** involves obtaining sensitive customer information with the purpose of misusing the data for financial gain.
- **Fiscal Fraud** describes fraud against the government, often through attacking government online channels, and includes theft, such as fraudulent claims for benefits, and evading taxes.[4]

2.4. The Global Cost of Cybercrime

Cybercrime results in significant costs across the globe but an accurate amount is hard to calculate because of the various crime types, methodologies and estimation processes. According to a 2011 study, the global cost of cybercrime was estimated to be $388 billion annually with direct cash cost of $114 billion including money stolen and spending on attack resolution. The indirect cost was estimated at $274 billion based on the value of time lost. [5]However, a 2009 study estimated the cost of lost intellectual property and expenditures for fixing the damage from data breach and theft to be as high as $1 trillion globally.[6]

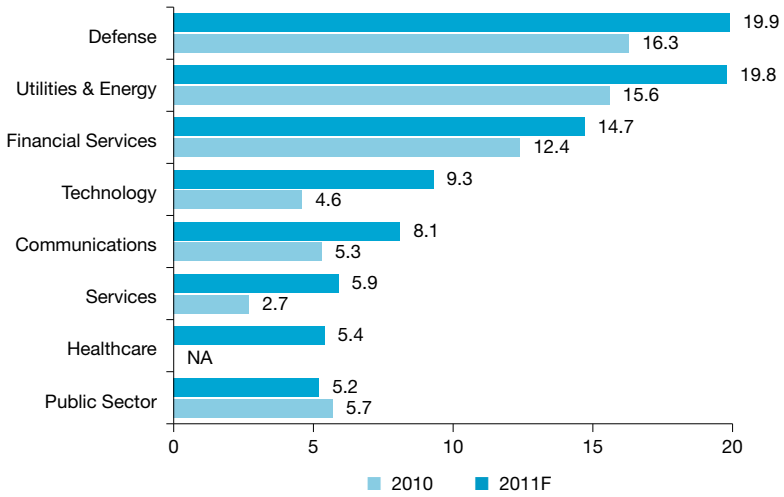
> "Thanks to the internet, the personal computer, and other technological advances, cybercrime is becoming a truly global phenomenon."
>
> *Cybercrime: The Growing Global Threat,* J. P. Morgan, 2011

And the numbers are growing fast. In a study of U.S. companies by the Ponemon Institute, the average annual cost of cybercrime is estimated to have increased by 22.6% from 2010 to 2011. Viruses, worms, and trojans are the most common and frequent type of cyber attacks. Around 90% of U.S. companies are estimated to suffer from malware attacks, 64% experienced web-based attacks, 44% experienced stolen or hijacked computing devices, and 42% experienced malicious code.[7]

[4] Ibid.
[5] Based on a survey conducted in 24 countries among adults 18-64, Norton Cybercrime Report 2011, Symantec, 2011, http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/
[6] Based on a survey of 800 CIOs conducted by Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) and McAfee, http://www.mcafee.com/us/resources/white-papers/wp-meeting-blended-threats.pdf
[7] Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies, Ponemon Institute LLC, 2011

Cybercrime is not limited to any specific industry. Defense, utilities and energy, and financial services remain the top industries in the U.S. suffering from cybercrime in terms of annual cost.

Exhibit 1: Estimated Average Annual Cost of Cybercrime per Company by Industry in the U.S. ($MM), 2010–11F



Source: Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies, Ponemon Institute LLC, 2011

IP theft is estimated to be the biggest contributor, with over 45% of total annual cyber crime cost to U.K. businesses, reflecting the fact that companies in IP-rich industries face a relatively higher risk from cyber crime.

Cybercrime is estimated to cost approximately £27 billion per year to the U.K. economy.[8] Approximately 80% or £21 billion is borne by U.K. companies. In Germany, the loss due to cybercrime was estimated at €90 billion in 2010 with a per case cost of €4000.[9]

According to a study[10] conducted in five countries—Australia, France, Germany, U.K., and U.S.—the average cost per company arising from data breaches reached $4 million in 2010, a rise of 18% from 2009.

Emerging economies are also affected by cybercrime activities. The total cost of cybercrime was estimated to cost around $25 billion in China, $15 billion in Brazil, and $4 billion in India during 2010.[11]

Clearly cybercrime has emerged as a serious threat to organizations across the globe. Although the actual financial implications of cybercrime remain difficult to measure, these statistics help quantify the possible risks and can help insurance companies understand the potential for loss from cybercrime activities.

[8] Cost of Cyber Crime, U.K. Cabinet Office and Detica, 2011
[9] "German Fear the Internet", Welt Online News Article, 2011, http://www.welt.de/print/die_welt/finanzen/article13461472/Deutsche-haben-Angst-im-Internet.html
[10] 2010 Annual Study: Global Cost of a Data Breach, Symantec and Ponemon Institute LLC, 2011
[11] Norton Cybercrime Report 2011, Symantec, 2011, http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

3. Prevention Versus Protection: The Case for Cybercrime Insurance

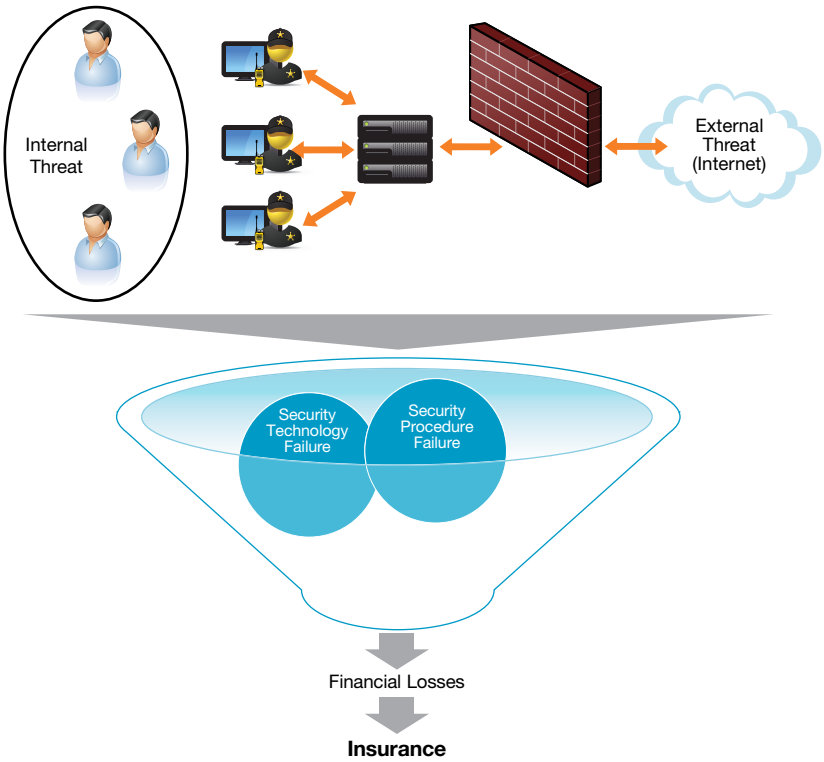
Although IT security technologies can provide a preventive measure against cybercrime, it is impossible to ensure complete protection. The very nature of cybercrime is ever changing with new schemes developing as rapidly as new technologies emerge. Despite the implementation of preventive measures, cybercrime attacks could still result in a substantial financial loss for any company. This financial risk, or exposure, can be mitigated in two ways[12]:

- Transfer the risk to an external insurance company by purchasing cybercrime insurance.
- Assume the risk internally by setting aside funds to compensate for the potential future loss. This is called self-insurance.

Self-insurance is the riskier of the two options since a company must accurately understand the risk in order to set aside appropriate funds. Instead, many companies are choosing to purchase cybercrime insurance, an emerging area for insurers.

Cyber crime insurance is a necessary hedge but not a substitute for solid business and IT systems that guard against breaches.

Exhibit 2: Mitigating Cybercrime Risk Using Insurance: How It Works



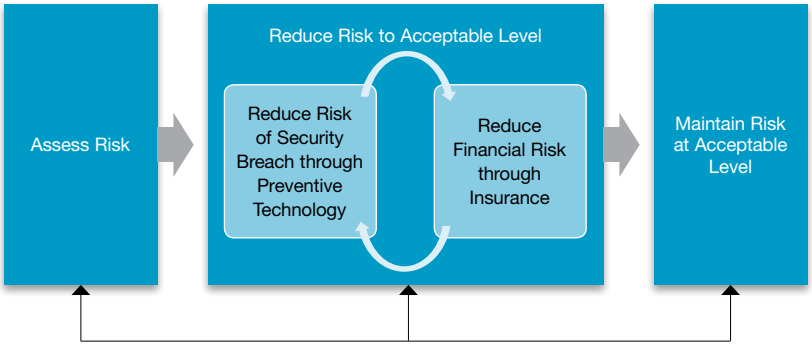
Source: Capgemini Analysis, 2012

[12] "CyberInsurance: A Market Solution to the Internet Security Market Failure", Willian Yurcik and David Doss, Illinois State University, http://www.cl.cam.ac.uk/~rja14/econws/53.pdf

3.1. A Cyber Risk Management Framework

In an article in *Communications of the ACM*, Gordon, Loeb, and Sohail suggested a three-step framework to manage the risk arising from cyber incidents.[13]

Exhibit 3: Cyber-Incident Risk Management Framework



Source: A framework for using insurance for cyber-risk management; Lawrence A. Gordon, Martin P. Loeb, Tashfeen Sohail; Communications of the ACM, Vol. 46 No. 3, Pages 81-85, 2003

Assess Risk

Companies must assess their current computer systems and determine the level of IT security. As a result of this process, a company can determine their risk exposure and potential loss in case of cybercrime.

Reduce Risk to Acceptable Level

Companies should look to reduce their risk by:

- Using preventive measures and technologies to reduce the risk of security breach.
- Transferring the risk by adopting cybercrime insurance coverage.

Maintain Risk to Acceptable Level

A combination of preventive measures and insurance allows a company to manage the cybercrime risk and maintain it at an acceptable level.

[13] A framework for using insurance for cyber-risk management; Lawrence A. Gordon, Martin P. Loeb, Tashfeen Sohail; Communications of the ACM, Vol. 46 No. 3, Pages 81-85, 2003

Insurance firms can only provide cover against cybercrime losses for which financial cost estimation can be achieved.

3.2. An Introduction to Cybercrime Insurance

In cybercrime, any loss is a result of two factors: a cyber attack and the failure of prevention mechanisms. Commercial general liability insurance is available for businesses to protect against potential losses such as property damage, workers' injury, or natural disasters. But traditional general insurance products do not cover cybercrime risk for a few reasons: the concept of cybercrime risk is relatively new, and the majority of commercial insurance provides coverage for tangible assets. Therefore, insurers must offer a specialized insurance policy to allow companies to transfer the risk arising from cybercrime.

In order to calculate premium rates and process claims after a cybercrime attack, an insurer needs to estimate the cost of loss from a cybercrime incidence. Since it is not easy to estimate non-financial losses such as reputation loss, companies who purchase cybercrime insurance can only transfer the calculable financial loss risk to the insurer.

Exhibit 4: Categories of Cybercrime Insurance

First-Party Insurance	Third-Party or Liability Insurance
▪ Protects against losses occurring directly to the insurance holder ▪ Covers mainly information asset damage including damage to the data, software, and systems of an organization ▪ Covers loss from business interruption due to software or system failure from cyber attack ▪ Includes cyber-extortion protection, which covers ransom costs and negotiating expenses	▪ Protects against claims for losses from another organization or individuals affected by a security breach ▪ Includes network security liability that covers losses due to the theft and misuse of data, including payout to victims as well as the recovery cost ▪ Includes network liability (downstream) protecting against denial of service attacks and forwarding of viruses ▪ Covers media liability including infringement and liability costs due to internet publishing, including websites, e-mail, instant messaging, and chat rooms ▪ May also include coverage against any liability of third-party loss arising from the negligence of an organization

Case Study: Insurance for Cybercrime from Chubb Group of Insurance

Chubb offers an insurance solution to cover cybercrime risk called CyberSecurity by Chubb[SM]. It is a combination of third-party liability insurance and optional first-party protection. Third-Party Liability includes coverage for:

- Disclosure injury, including lawsuits alleging unauthorized access of private information.
- Content injury, including suits arising from intellectual property infringement, trademark infringement, and copyright infringement.
- Conduit injury, including suits arising from system security failures that result in harm to third-party systems.
- Impaired-access injury, including suits arising from system security failure resulting in your customer's systems being unavailable to their customers.
- Reputational injury, including suits alleging disparagement of products or services, libel, slander, defamation, and invasion of privacy.

First-Party Protection covers:

- Notification expenses to customers affected by a data leak.
- Loss from business interruption.
- Cost of data recovery.
- Crisis management expenses, including the cost of public relations consultants.
- Extortion expense, including the cost of a professional negotiator and ransom payment.
- E-communication loss, extended to networks outside of your company's system.

Source: Cybersecurity by Chubb, Chubb Group of Insurance, http://www.chubb.com/businesses/csi/chubb10600.pdf

4. Key Challenges for Insurers

Cybercrime risk is a relatively new type of commercial risk and its inherent nature poses a number of challenges. There are also a number of external challenges that can result in a barrier to widespread availability of this type of coverage.

4.1. Challenge #1: The Inherent Nature of Cybercrime Risk

Predicting the probability of occurrence and determining the business impact is required for risk measurement and assessment. Since cyber attacks or security breaches may lead to a variety of business consequences, it is very **difficult to quantify the impact**.

Cybercrime is a relatively new concept and insurance firms are still building standard methodologies and financial models to **determine an appropriate price** for this risk. A **lack of historical data** is one of the foremost issues faced while determining the premium rate of an insurance policy and deciding on whether to underwrite the risk.

Because a new vulnerability can be exploited simultaneously across many companies worldwide, **cyber security incidents are highly linked** and can lead to huge losses across the globe. Additionally, cyber risks are **highly interdependent** and one compromised system may increase the vulnerability of other systems in a single company. For large multi-national companies like financial services institutions, cyber security incidents can open up all software, IT systems, and infrastructure to attack.

Insurers may find it difficult to **monitor changes to the risk** of a particular cyber insurance policy. For example, a company may reduce investments in IT security which would increase cybercrime risk during the policy cover.

4.2. Challenge #2: The Lack of Standards, Metrics, and Governance for Cybercrime Insurance

The insurability of cyber risks is impacted by a **lack of standard legal definitions** of cyber liability across the globe. The internet is global but the jurisdiction of country laws is restricted by geographical limits. This results in confusion over applicability of laws for any cross-border attacks, which is a common feature of cyber attacks.

Additionally, the possibility of large losses means there is **limited reinsurance** across the cyber insurance industry. Insurers and reinsurers are afraid of a **cyber-hurricane**[14]—a major disaster involving simultaneous attacks worldwide, resulting in many claims.

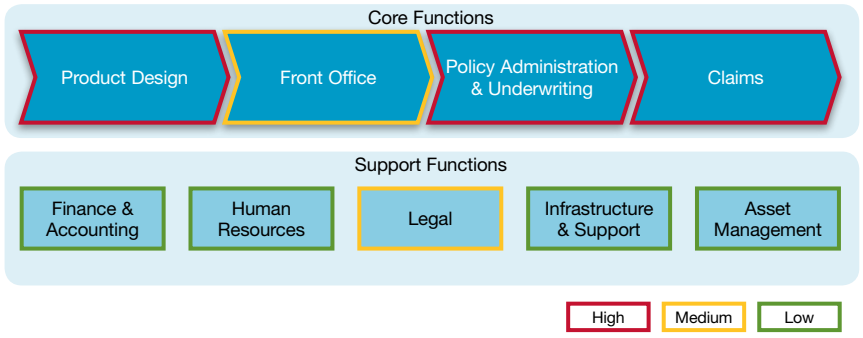
[14] Cyber-Insurance Metrics and Impact on Cyber-Security, Whitehouse (U.S.) Whitepaper, 2006

While IT security solution providers work to provide protection from all vulnerabilities, every year new weaknesses are uncovered and exploited in cybercrime attacks. A lack of understanding of IT systems and security standards by insurers can lead to miscommunication. Therefore, insurers must establish a standard set of security metrics to quantify the security level at each insured company.

4.3. The Impact of Cybercrime Insurance across the Value Chain

Emerging products to address cybercrime risk will impact most areas of the insurance value chain, from product design to claims. The areas of most impact will be product design, policy administration, underwriting and claims, but the new risk will also affect front office and legal.

Exhibit 5: Impact of Cybercrime Insurance across the Value Chain



Source: Capgemini Analysis, 2012

High Impact Area #1: Product Design

While launching new policies and products, insurers must identify standard definitions, terms of use, criteria for eligibility, and design of a policy document while adhering to local regulations. Insurers must also determine a set of premium rates for standard coverage policies and configure the new product across all core processing systems.

High Impact Area #2: Policy Administration & Underwriting

Offering cybercrime insurance will have a significant impact on an insurer's underwriting processes. Insurers will need to define procedures to:

- Analyze the risk of covering a particular company.
- Assess the level of IT security in place.
- Determine the price of covering the cybercrime risk.

Apart from pre-issue activities, insurers also need to manage external factors such as regulatory changes and any differences that may affect IT security for the insured. For example, implementation of any new system; change in security procedures; or expansion of infrastructure can all change the risk of cybercrime.

High Impact Area #3: Claims Processing

Claims processing and investigation for cybercrime insurance policies require significant input from technology and IT security experts. Claims need to be assigned to a team that includes claims adjustors, IT professionals, and security industry experts. Procedures and models must be defined to calculate the potential loss from any cybercrime incident, especially in case of third-party liability. Insurers also must assess whether existing fraud detection and prevention capabilities are applicable to cybercrimes or if new ones are needed.

Medium Impact Area #1: Front Office

Today's insurance companies are experiencing significant growth in the channels through which they sell insurance. Cybercrime insurance products can be sold through many of these emerging channels or an insurer may choose to use an existing distribution network. Either way, sales people, agents, and customer service representatives will require training on cybercrime and legal issues to sell this new insurance.

Medium Impact Area #2: Legal

Legal counsel at insurance companies will need to define legal terms related to cybercrime and manage litigation for the new cybercrime insurance products.

5. Key Recommendations

Cybercrime insurance involves a combination of knowledge of both insurance and technology so insurers planning to offer these products need a wide range of solutions and services across the insurance value chain.

5.1. IT Recommendations

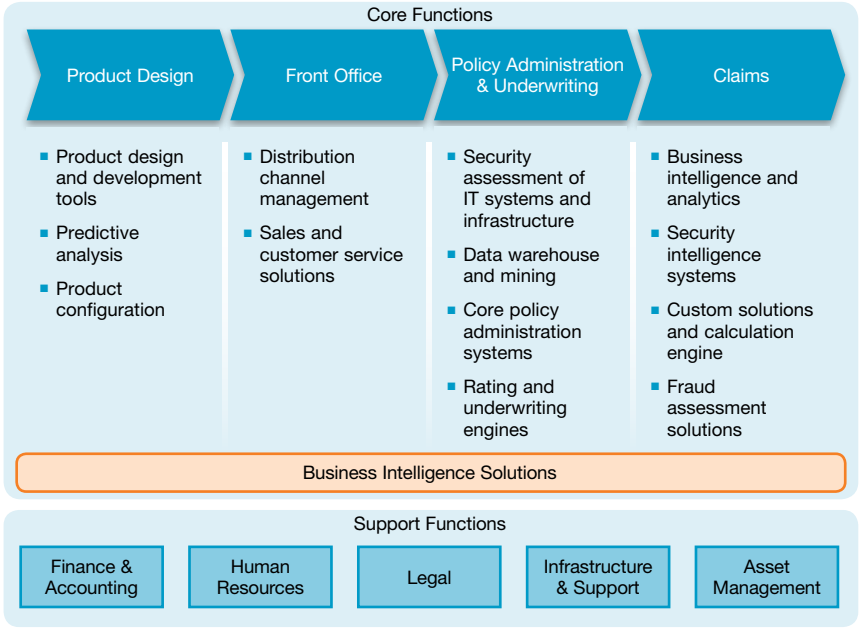
Product Design

- Leverage existing product design and development tools and configurations to introduce and configure the new type of policy.
- Use predictive analytics and business intelligence tools to determine standard premium rates.
- Consider using the experience of IT security solution providers in managing cybercrime cases.

Front-Office

- Train sales on new sales and customer service solutions in addition to legal and cybercrime topics.
- Use distribution channel management tools to increase selling effectiveness.

Exhibit 6: Technology Requirements Needed to Support Cybercrime Insurance Products



Source: Capgemini Analysis, 2012

Policy Administration & Underwriting

- Plan and implement required modifications to existing systems such as core policy administration system or rating and underwriting engines.
- Create a new data warehouse to collect information from insured companies, IT security firms, and historical cybercrime incidences.

Claims Processing

- Leverage business intelligence, analytics, and data mining to measure claims cost.
- Consider developing a custom solution to determine loss arising from a particular claim.

5.2. Business Recommendations

Adding any new product can result in IT changes for an insurer, but due to the nature of cybercrime insurance a large number of guidelines and processes are also affected.

Pre-Policy Issue

Before issuing cybercrime insurance policies, insurers must do a security assessment of the insured. This assessment should study computer systems, infrastructure, and networks to locate any potential security vulnerabilities and risks. Insurers may look to develop the assessment capability in-house or utilize specialized external vendors. The process should include evaluating the level of security procedures and policies.

Exhibit 7: What to Evaluate in a Cybercrime Security Assessment

Physical Security	Is proper identification and screening of visitors required for all insured locations?
Incident Management Procedures	Is there a mechanism for efficiently managing IT security incidents/violations and related risk management?
Network & Application Security	Does the insured use firewalls, password security, and perform vulnerability tests?
IT Security Audit	Is there a mechanism for auditing the adherence to various IT security policies?
IT Security Expertise	Is a dedicated IT security team available with appropriate expertise?
IT Security Awareness Programs	Are employees and business partners trained on the organizational IT security policy and guidelines?

Source: Capgemini Analysis, 2012; Exploring Costs, Capital Requirements and Risk Mitigation, Allan Grody, 2005

Insurers also must confirm the implementation of necessary prevention and monitoring systems at the insured. This might include a list of recommended industry solutions that serve as precondition to coverage.

Post-Policy Issue

Apart from traditional policy administration steps, once a cybercrime insurance policy has been issued, insurers should reassess IT security at the insured for any changes that might affect the policy. For example, system changes, regulatory changes, or innovations in the IT security industry could all result in a need to reassess existing cybercrime insurance policies. Security intelligence tools can help insurers monitor ongoing changes and the health of security solutions.

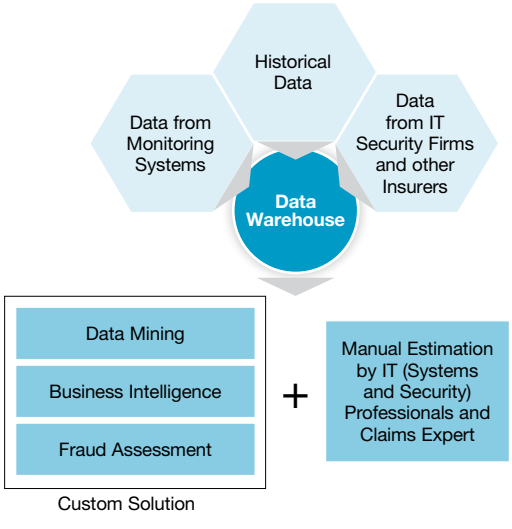
Measuring Claims Costs

Insurers should utilize both technology solutions and expert professional assistance to estimate the claims cost of cybercrime incidences. To estimate the business impact when a cybercrime event occurs, insurers need to have or collect the following information:

- The state of the insured's IT systems at the time of the attack and the impact on other related processes.
- Historical data about security incidences in the same company, other companies in the same industry, or across all industries.
- From IT security firms, information on the security systems and technology that is used by the insured.
- From other insurance companies, data to help analyze a wide range of cyber attacks and vulnerabilities seen across various companies.

In general, claims estimation is more art than science so insurers will need to combine custom tools and manual estimation processes.

Exhibit 8: How to Measure Cybercrime Claim Costs



Source: Capgemini Analysis, 2012

6. Conclusion

To address the risk of cybercrime, companies should use a combination of technology for prevention and insurance for mitigation. Through cybercrime insurance, companies can transfer the financial consequences of IT security incidents to an insurer.

As cybercrime risk is a relatively new type of commercial risk, the challenges faced by the insurer may result in a barrier to widespread availability of this type of insurance coverage. Insurers will also experience a significant impact across the insurance value chain.

Thus, insurance companies offering coverage for cybercrimes will need to make adjustments to both IT and business processes. Insurers need to find the right balance between developing in-house capabilities and seeking assistance from external professionals to effectively manage the insurance life cycle for cybercrime insurance policies.

References

1. Internet Crime Complaint Center (IC3), U.S., http://www.ic3.gov/
2. SearchSecurity.com, http://searchsecurity.techtarget.com/
3. McAfee Security, http://www.mcafee.com/
4. Symantec Corporation, http://www.symantec.com/
5. Oz Forex Foreign Exchange Service, http://www.ozforex.com.au/
6. *2010 Internet Crime Report*, Internet Crime Complaint Center (IC3), 2011, www.ic3.gov/media/annualreport/2010_ic3report.pdf
7. *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies*, Ponemon Institute LLC, 2011, http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf
8. *First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies*, Ponemon Institute LLC, 2010, http://www.arcsight.com/library/download/ponemon-2010-cost-of-cyber-crime-study/
9. *2010 Annual Study: Global Cost of a Data Breach*, Symantec and Ponemon Institute LLC, 2011
10. *Norton Cybercrime Report 2011*, Symantec, 2011, http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/
11. *Q&A: Cyberinsurance Fundamentals For Security And Risk Professionals*, Forrester Research, 2011
12. *RSA 2011 Cybercrime Trends Report*, RSA, 2011,
13. *The Cost of Cyber Crime*, U.K. Cabinet Office and Detica, 2011, http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime
14. *Cybercrime: The Growing Global Threat*, J.P.Morgan, 2011
15. *2011 Threats Predictions*, McAfee Labs, 2011
16. *Business Counts The Cost Of Cyber Crime*, The Independent Article, http://www.independent.co.uk/news/business/analysis-and-features/business-counts-the-cost-of-cyber-crime-2236158.html, accessed on 10th Sept, 2011
17. *ISAlliance on Finance Sector Cybersecurity*, Infosecisland.com Article, https://www.infosecisland.com/blogview/3973-ISAlliance-on-Finance-Sector-Cybersecurity.html, accessed on 10th Sept, 2011
18. *Using Cyber-Insurance to Improve Cyber-Security: Legislative Solutions for the Insurance Market*, ISA Whitepaper, http://thehill.com/images/stories/whitepapers/pdf/ISA_CyberSecurityCyberInsurancePaper.pdf, accessed on 10th Oct, 2011
19. "*CyberInsurance: A Market Solution to the Internet Security Market Failure*", Willian Yurcik and David Doss, Illinois State University, http://www.cl.cam.ac.uk/~rja14/econws/53.pdf, accessed on 10th Oct 2011
20. "*McAfee: Corporate Espionage Is the Currency of Cybercrime*", PC World Article, http://www.pcworld.com/businesscenter/article/223483/mcafee_corporate_espionage_is_the_currency_of_cybercrime.html, accessed on 5th Sept, 2011

21. *Cybercrime in Europe: Recent Legal & Policy Developments*, Cedric Laurant, 2010, http://www.fecomercio.com.br/arquivos/arquivo/Cybercrime%20in%20Eurpe%20-%20Cedric_6zd9z7aqaa.pdf

22. *Cyberinsurance in IT Security Management*, IEEE Computer Society, 2007, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4218551

23. *The Evolution Of Cyberinsurance*, University of Illinois at Urbana-Champaign, 2006, http://arxiv.org/abs/cs.CR/0601020

24. *Cyber-Incident Risk in Canada and the Role of Insurance*, ICLR Research, 2004, http://www.iclr.org/images/Cyber-Incident_Risk_in_Canada_and_the_Role_of_Insurance.pdf

25. *A Framework for Using Insurance for Cyber-Risk Management*, Communication of ACM, Volume 46, 2003, http://www.cc.gatech.edu/classes/AY2008/cs4235b_fall/Group3/FrameworkUsingCyberInsurance.pdf

26. *The Financial Impact of Cyber Risk:50 Questions Every CFO Should Ask*, American National Standards Institute and Internet Security Alliance, 2008, https://netforum.avectra.com/temp/ClientImages/ISA/05042350-fb9b-41bd-9405-8b122960c5c1.pdf

27. *Using Cyber-Insurance to Improve Cyber-Security: Legislative Solutions for the Insurance Market*, Internet Security Alliance (ISA) Whitepaper, http://thehill.com/images/stories/whitepapers/pdf/ISA_CyberSecurityCyberInsurancePaper.pdf, accessed on 15th Sept, 2011

28. *Cyberinsurance as a Market-Based Solution to the Problem of Cyber Security – A Case Study*, University of Illinois at Urbana-Champaign, 2005, http://infosecon.net/workshop/pdf/42.pdf

29. *Cyber-Insurance Metrics and Impact on Cyber-Security*, Whitehouse U.S., http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf, accessed on 15th Oct, 2011

30. "*How Cyber Insurance Might Ease Your (Network) Insecurity*", Microsoft, http://www.microsoft.com/business/en-us/resources/ArticleReader/website/default.aspx?Print=1&ArticleId=Smallbusinescyberinsurance&fbid=u3k-auyhhed, accessed on 10th Nov, 2011

31. *Interdependent Security: The Case of Identical Agents*, National Bureau of Economic Research, http://www.nber.org/papers/w8871.pdf

32. *How Will You Survive a Data Security Breach*?, Chubb Group of Insurance Companies, http://www.chubb.com/businesses/csi/chubb10600.pdf, accessed on 10th Nov, 2011

33. "*How to recognize phishing email messages, links, or phone calls*", Microsoft, http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx, accessed on 20th Nov, 2011

34. "*German Fear the Internet*", Welt Online News Article, 2011, http://www.welt.de/print/die_welt/finanzen/article13461472/Deutsche-haben-Angst-im-Internet.html, accessed on 15th Oct, 2011

35. "*What About 'Cyber-insurance*'?", CIO New Zealand Article, http://cio.co.nz/cio.nsf/depth/F982BE098F967D5ACC2576B900056F2B, accessed on 15th Oct, 2011

About the Authors

Amit Jain is a Senior Consultant in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. He has over four years of experience in strategy, business, and technology consulting for financial services clients across insurance, banking, and capital markets.

Sridhar Kalyanam is a Senior Manager within Capgemini's insurance practice. He has over 24 years of experience in insurance and banking domains across IT consulting, project management, operations, and business for clients across the globe.

The authors would like to thank **Chirag Thakral**, **David Wilson**, **Sree Rama Edara**, and **William Sullivan** for their contributions to this publication.

For more information, visit **www.capgemini.com/insurance** or e-mail **insurance@capgemini.com.**

About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™.

The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients.

Present in 40 countries, Capgemini reported 2011 global revenues of EUR 9.7 billion and employs around 120,000 people worldwide.

Capgemini's Global Financial Services Business Unit brings deep industry experience, innovative service offerings and next generation global delivery to serve the financial services industry.

With a network of 21,000 professionals serving over 900 clients worldwide, Capgemini collaborates with leading banks, insurers and capital market companies to deliver business and IT solutions and thought leadership which create tangible value.

For more information please visit **www.capgemini.com/financialservices**

Rightshore® is a trademark belonging to Capgemini