The good, the bad and the careless
An overview of corporate cyber risk
The good, the bad and the careless

Over the past decade or so, the Internet really has changed everything. Mostly for the good. Yet it has also opened up some major cyber risks – mainly to theft and accident. Virtual crime, and virtual mishaps, can lead to real-life losses of property, income and reputation, as well as increased liability. Moreover, these losses can be interconnected; one loss can trigger another, like a row of tumbling dominoes.

Consider the U.S. mass merchandiser Target. In late 2013, thieves reportedly broke into the company’s network using logins taken from another company servicing its heating and air conditioning system, accessed its payments system, and then stole payment card details for 40 million customers.¹ The breach could cost Target hundreds of millions of dollars including legal, consulting and credit-card monitoring services. The price tag for lost consumer confidence is not known.

Zurich Insurance Company Ltd (Canadian Branch) has made cyber-risk a priority. We’re researching it, lobbying about it, offering expertise and insurance coverage. You can find an overview at our website, http://www.zurichcanada.com/can/en/solutions/security-privacy-solutions/cyber-thought-leadership.htm

This white paper is aimed at corporate customers – either existing or potential – and anyone else who shares our interest in this growing problem. It is meant to give non-experts an overview of cyber risk, including:

• Who are the perpetrators, who causes cyber risk?
• What do they do, how does it happen?
• Just what is at risk?
• What can be done to protect against it?

Cyber power: the good, the bad and the careless

We don’t work or live the way we used to. Communication and storage of information has changed dramatically; technology rules. To a degree many of us once would have found inconceivable, our lives have gone digital. Digital or virtual technology is an amplifier. It enables its users to do far greater things than they could without it. That includes great good and great bad.

Much research and attention has been focused on the good. This report, however, is focused on the bad – lesser-known, but still very important. It starts with a look at the perpetrators. They fall into two categories: people who threaten companies for reasons of greed, malice or hostility; and those who endanger others through their own carelessness.

**Who are the real cyber villains?**

Intentional threats from the cyber world fall into two basic categories. First are criminals and vandals who want to rob, defraud or otherwise harm companies or their customers. Second are spies or soldiers, who when snooping or attacking on behalf of a government, might hit a company as part of their collateral damage.

**Cyber thieves and con artists**

Perhaps ironically, you can find some of these easily on the Internet. Just look at the ‘Cyber’s Most Wanted’ list posted by the U.S. Federal Bureau of Investigation. Almost always the charges are either theft – of money or data – or fraud.

Who are these people? As it turns out, most do not fit the popular misconception of a young computer geek working alone. According to a 2012 study by BAE Systems and the London Metropolitan University, 80 percent of cyber crime is the work of professional criminals. This is no hobby; this is their job.

In most cases cyber criminals work for an organization, typically numbering to about five or six members, with sometimes up to around 15. Many are based in the former Soviet Union, with like-minded groups located in the Americas, China, India and Nigeria. These groups are not – at least not yet – as large or established as traditional organized crime syndicates. They are more nebulous, informal and short-lived; often they are run as a sort of ‘project team’ composed of freelancers.

Also against stereotype, cyber thieves and cons are not especially young. Their average age is between 26 and 35, according to the BAE-London Metropolitan University study. Nor are they all aces of IT. Of course there are a few about, but the rest are ordinary 9-to-5 criminals. This is mainly due to a ‘deskilling’ of digital crime made easier by the availability of ‘crimeware’ that can be bought off the shelf and used by anyone. These toolkits offer everything from readymade viruses to exploit the vulnerabilities of individual systems to ‘bot-nets,’ basically ‘do-it-yourself’ malware construction kits or ‘exploit-hack packs’ and other tools that reap information without users being aware their computer is infected.

---


4 Ibid.
Virtual vandals: the hacktivists
In the real world, these are the people who spray graffiti or protest against corporate greed using illegal means. Now they are a multi-channel operation with an online presence.

Depending how one looks at it, so-called hacktivists can be classified anywhere from attention-seeking troublemakers to ‘freedom fighters.’ They portray themselves as Robin Hoods of the Internet, fighting the corrupt powerful for the rights of the innocent powerless. Whatever they are, their operations often fall within a gray area of the law, somewhere between legal protest, civil disobedience and criminal mischief.

Probably the best known are WikiLeaks and Anonymous.

Collateral damage to corporations: spies and warriors
Governments, for ill or good, have played an active role in the development of technology. ARPAnet, the precursor of today’s Internet, was originally designed by the U.S. Department of Defence. The extent of cyber surveillance and cyber attacks are not general public knowledge. Various reports have suggested the involvement of governments of China, Israel, the U.S. and others.

Unforced errors: carelessness (or malice)
To get an idea of potential sources of cyber threat, look around the office or even in a mirror. Accidents happen, sometimes with valuable data. This is primarily due to carelessness, according to market research. Nonetheless, as many as one-fourth of such incidents could be intentional sabotage by disgruntled employees that are then passed off as honest mistakes.

The three faces of cyber risk
Meet the terrible trio: theft and fraud; intentional harm, and accidents. These are the main forms of cyber risk. And there is even a fourth, hybrid sort of danger. That is when a series of risks become linked, creating a sum of damage greater than its individual parts.

One study has estimated that cyber crime’s annual cost to the global economy — each year — might be USD 400 billion or possibly more. It is a war that is escalating, as both sides improve their game. The stakes are high.

Hacking to steal
Sadly, it is amazingly cheap and easy to buy stolen credit cards. A Russian-based website offers stolen card-details for less than five U.S. dollars each. Ricardo Villalobos, founder and CEO of security consultants EasySolutions, dubs such online sites, due to the ease at which information can be obtained, as “the Amazon of the cybercrime economy.”

And it’s not just credit cards that are on sale. Cyber thieves will take almost anything that they can use to impersonate a valid customer: passwords, personal identification numbers, tax or benefits codes. From that point on, they work in much the same way as other burglars, stealing relatively small sums of cash or goods (maybe up to USD 100 to USD 200 per transaction) until the impersonated person finds out and changes their details.

Thieves are out for data, too. For instance, in 2014, the U.S. accused five Chinese military officers with cyber hacking that enabled them to steal trade secrets, including from Westinghouse, as the company was negotiating with China to build a nuclear power plant there.

How easy is it to crack a password?
Simple passwords may be cracked in seconds or even a fraction of a second. Like other technology, password-cracking tools have evolved. It might be simply an approach that tries out different combinations using ‘guessing’ attacks, with the most susceptible likely to be opened in seconds, or even fractions of seconds.

There is a library of research available on the vulnerability of different types of passwords and tools to crack them, some with fanciful names like ‘John the Ripper.’ But, while sophisticated tools are available, it is even possible to use a popular gaming console to achieve the same purpose.
At first, cyber thieves worked mainly by brute force. In 1994, a Russian mathematician, Vladimir Levin, conducted what is thought to be the world’s first ‘virtual’ bank robbery. Levin led computers at Citibank to send money to accounts in Finland, Israel, and San Francisco.\(^{10}\)

In the face of this, Citibank and others went on to invest major sums in firewalls, password-protection, encryption and all the other trappings of secure communication. And clearly, these present a formidable barrier to today’s hackers. Rather than engage in a digital arms race, many of them have turned to a softer target: guileless humans.

**Modcons – social engineering**

“I’m here to check the system,” says the non-descript type in jeans and a T-shirt claiming to be from the IT department. “I misplaced my password,” says a voice professing to be the boss from the other end of a crackling phone line. “Urgent,” states the phony email, “please resend those pricing calculations.”

Social engineering is the catch-all term for cyber cons and scams. Although it seems incredible, some people really do fall for the Nigerian emails asking for bank transfers. More refined are what the U.S. FBI calls ‘ransomware’ or ‘scareware’. For instance, somebody surfing the Internet suddenly gets a pop-up box that says the PC is virus infected, and then offers ‘antidote’ software for purchase. Fiendishly, the so-called antidote then actually carries an infection to the machine.

Scams take advantage of human nature: the willingness of most people to trust others and their desire to avoid conflict or embarrassment. People are much easier to manipulate than technology. The man whom Wired magazine called a ‘legendary cracker,’ Kevin Mitnick, might be a shining example of this. According to media accounts he was able to get into systems in part through his ‘social engineering’ skills. With accents, impersonations and similar low-tech ‘skills’ he could convince unsuspecting employees to divulge information that he used to hack into systems. The man described by some as a ‘prankster’ or a ‘recreational hacker’ was arrested in 1995 and convicted of breaking into computers of some large corporations. Today he charges for his work as a security consultant.\(^{11, 12, 13}\)

**Theft by any other name: surveillance**

It’s not just conventional hackers involved. This was made most obvious by Edward Snowden, who in mid-2013 leaked the eavesdropping being conducted by the U.S. National Security Agency. A few years prior, a Canadian group detected what it believed to be a cyber-espionage operation, thought to be based mainly in China, which had infiltrated high-value targets including foreign ministries, embassies, international organizations, news media, and nongovernmental organizations.\(^{14}\)

---


Spam and viruses
Junk mail’s virtual equivalent is simply enormous. More than two-thirds of all emails are spam, based on data for 2013 compiled by IT security firm Kaspersky Lab. ¹⁵ Not all of it is criminal, of course. But a significant minority of spam is sent with intent to steal or defraud.

Particularly devious is spam that comes with a heinous payload – a link to a dodgy website, or a virus waiting to infect your network. The latter can cause all sorts of problems: crashing a computer, stealing confidential data, spying on users, even using the email to send out more spam, usually without the user even knowing.

Most years have seen three to five virus scares that cause major disruptions and shutdowns. Perhaps best known were ‘Mydoom’, which infected 250,000 computers within days in 2004, and the ‘ILOVEYOU’ bug that hit on a similar scale in 2000.

The hurt factor
Causing trouble is the second main type of cyber risk. Intentional harm falls into two predominant types: inside jobs, and hacktivism/cyber-war.

Inside jobs
The problem takes on a whole new dimension when an unhappy employee has computing access and skills. Precise statistics about retribution by employees are unavailable, not least because most cases are settled in private. One study found that 70 percent of insider incidents were handled internally without legal action.¹⁶

For angry employees, where there’s a will, there’s a way.
• The sacked technician: a computer technician was charged with sabotaging the computer system of Forbes Inc. in retaliation for his being fired. Media, quoting law enforcement officials, said the attack caused a crash that cut off employees from the computer service, and caused more than USD 100,000 “worth of havoc.”¹⁷

• A technician at NDB, Switzerland’s Federal Intelligence Service downloaded classified information including possibly from British and U.S. intelligence agencies and attempted to sell it, after carrying it out of government buildings in a backpack. It is possible he became disgruntled after his advice on operating data systems was not taken seriously, one report suggested.¹⁸

Hacktivism and cyber war
Both hacktivists and cyber warriors can assault organizations. The threat is much the same; they just work for different people.

Hacktivists are typified by a hacker collective called Anonymous that, thanks to several attacks, is anything but ‘anonymous’.

• Operation Japan: in 2012, a Twitter® feed associated with Anonymous temporarily took down several Japanese government websites in what was reported to be a protest against a new copyright law in that country, which Anonymous claimed would reduce privacy.\textsuperscript{19}

• Out in the open: one year prior, Aaron Barr, CEO of a U.S. security firm, threatened to name the leaders of Anonymous. Within a day, Wired magazine reported that Anonymous had managed to infiltrate Barr’s company’s website and take it down, replacing it with a pro-Anonymous message. It compromised his company’s email server and posted over 40,000 emails on a public platform. It even claimed to have remotely ‘wiped’ his iPad.\textsuperscript{20}

Cyber-warriors do not attack only governments.

• New York Times takedown: for half a business day in August 2013, ‘All the News that’s Fit to Print’ wasn’t. A group calling itself the so-called Syrian Electronic Army crashed the newspaper’s website, presumably to protest its coverage of that country’s armed conflicts. The group also attempted similar attacks on the respective websites of CNN, the Financial Times and the Washington Post.\textsuperscript{21}

• Corporate heist funds terrorism: in 2011, four people were arrested in the Philippines for hacking into accounts of AT&T customers, and diverting the money to a group that financed terrorist attacks in Asia. The Philippines police said the scheme cost USD 2 million, and preyed on telephone accounts protected by weak passwords.\textsuperscript{22}

• Worm in the machine: in 2010, a computer worm, ‘Stuxnet,’ apparently targeting Iran’s nuclear program, was designed in a way that could send nuclear centrifuges out of control. Such changes could cause centrifuges, used to enrich uranium for reactors or bombs, to blow apart.\textsuperscript{23}

**Accidents will happen**

Accidents will happen, and as computing and communications networks grow, so too does their likelihood. Yesterday’s mistakes were possible on a limited set of terminals and log-in points; today’s errors can happen on billions of devices operating just about anywhere.

How much damage can employees do?

• Leak confidential data: governments, hospitals, banks, universities and other guardians of confidential data (academic results, health records, mortgage applications, benefits and financial identifiers) unwittingly give these away with depressing regularity. One government agency posted the social security numbers of three million people on its website for over a year. A major bank leaked records for more than one million of its customers, because a number of its own staff had, for years, used shared log-ins and passwords.


\textsuperscript{20} Anderton, Nate. ‘How One Man Tracked Down Anonymous – And Paid a Heavy Price.’ 10 February 2011.


‘Risks multiplied’ – when dangers cascade

A less obvious, but potentially more dangerous threat is when all of the risks join up.

As a 2014 report by the Atlantic Council and Zurich Insurance Group notes: “Just imagine if a major cloud service provider had a ‘Lehman moment,’ with everyone’s data there on Friday, and gone on Monday. If that failure cascaded to a major logistics provider or company running critical infrastructure, it could magnify a catastrophic ripple running throughout the real economy in ways difficult to understand, model or predict beforehand. Especially if this incident coincided with another, the interaction could cause a crash or collapse of much larger scope, duration and intensity than would seem possible – similar to the series of events that struck the financial system in 2008.”

Even worse is a scenario that has led some experts to speak of a ‘Cybergeddon:’ The Internet turns into a battleground between thieves and thieved, aggressors and victims, predators and prey. It becomes such a dangerous place that ordinary people and companies cease to use it.

Cybergeddon, indeed. Because can you, or anybody imagine life today without the Internet?

What (and how much) is at risk?

Do you use popular online platforms? How about common consumer software? What about popular retailers, online auction sites, electronic game makers, supermarkets, telecommunications and online search engines. Companies in all these categories, highly regarded for their IT savvy, have been hacked.

According to some reports, as many as 400 million customer accounts of these companies were ‘compromised’ in recent years. Their user registrations and details have been acquired by unauthorized third parties. A typical result is that of a Tesco Clubcard (supermarket loyalty card) member that the Telegraph newspaper reported in early 2014. When the member went to buy an iPad, she planned to pay with saved-up membership points worth approximately USD 200; however, Tesco told her she had no points at all. As it turned out, the points had been stolen – and presumably used by hackers. Tesco declined to reveal how many accounts were compromised. Reports of the fraud included several in which victims have lost money more than once and where, in the case of the customer described here, “they changed their passwords after the first attack.”

---


For companies, the cost of cyber crime can be enormous. One study by the Ponemon Institute estimated an average ‘annualized’ cost of cyber crime for over 200 organizations of USD 7.2 million per year. Business disruption represents the highest external costs (fines, legal cases, stolen property, etc.), followed by costs due to losing information.27

Of the over 5,000 companies in 99 countries polled by PricewaterhouseCoopers for its 2014 Global Economic Crime Survey, one in four said they had experienced cyber crime, with 11 percent of those reporting financial losses greater than USD 1 million.28

Obviously some of the losses will be property, tangible or intangible. But that is truly the tip of the iceberg. Suffering a data breach – whether criminal or accidental – can trigger a raft of other charges, including liability and fines from regulators. It can also interrupt business and damage your reputation.

Seven ways to lose – as the unlucky Tesco Clubcard member learned, cyber-criminals will put stolen identities to work for them to steal cash or merchandise. Unfortunately for the hacked company, things can get worse. According to Tim Stapleton, Zurich’s Deputy Head of Professional Liability, there are another seven ways to lose.

Forensic investigation – like it or not, an investigation usually must be undertaken to understand what happened and how. Third-party investigators generally charge fees in the USD 100 to USD 1,000/hour range.

Notifying the victims – many governments require that ‘owners’ of breached data (i.e., customers or business partners of the breached company) be told about it. Even if this is not mandatory, for most businesses it is probably good practice to do so. Costs can run to USD five to USD 50 per notice, says Zurich’s Tim Stapleton.

Call centre – in notifying the victims, best practice among many breached companies is to provide an ‘Answerline’ phone number that customers can ring for information and support.

Post-theft monitoring – so, are the hackers going to use my name, email, credit card or not? As a form of restitution, many breached companies monitor this for the victims. And for cases where such information is used, they often offer to ‘restore’ the data to its proper owner. All told, this can cost USD 10 to USD 30 per victim.

Mitigation of image damage – data leaks can be similar to physical leaks of, say, oil or chemicals or pollutants, in that they trigger public indignation, and not just among victims. Most companies are not experienced in dealing with public anger, and so find it best to involve public relations experts to help.

Legal defence costs, settlements and indemnity payments – if the breach is serious enough, some victims are likely to sue for damages. According to a study of insurers by security firm NetDiligence, the average claim payout for a breach was USD 954,253. The average cost for crisis services was USD 737,473, and the average cost for legal defence was USD 574,984, while legal settlement cost on average USD 258,099.

### What hackers want
The most-common types of information stolen in a data breach are:

- Real names
- Birthdates
- Government ID numbers (e.g., for benefits or pensions)
- Home address
- Medical records
- Phone numbers
- Financial account authorization details
- Email addresses
- User names, passwords
- Insurance details26

---


Incidents caused by ‘improper actions or negligence’ by the affected organization tended to be slightly higher than costs related to simple errors, such as staff mistakes or something that an external provider did. “The exception is hacking incidents, which, while not directly caused by the affected organization, were extremely expensive.”

Fines and penalties – losing personal data can be a civil or legal offence. The fines or penalties can range from as little as USD 100 to more than USD 1 million, Stapleton estimates.

**Business interruption and reputation damage**

And then there is that matter of image. Although the precise value at risk can be difficult to quantify, in most cases one thing is certain: losing it can hurt dearly. Consider potential customers of retailer Target, cited earlier in this study. “If you Google them to do some shopping, and instead you’re flooded with news of their data breach, it just might put you out of a buying mood,” said Lori Bailey, Global Head of Management & Professional Liability at Zurich.

**Protecting against cyber risk: resilience is key**

When it comes to cyber security, even giants of the Internet may have feet of clay. Data breaches, virus attacks, scams and theft have struck the most sophisticated of organizations. Nobody is truly immune.

This is unlikely to disappear anytime soon. Motivated cyber criminals, hackers and cyber warriors are committed to an ongoing arms race, steadily improving their tools and methods of thieving, conning and harming. Meanwhile, accidents are sometimes going to happen.

Corporations are therefore advised first to take precautions, both internal and external, and at the same time to focus on resilience, the ability to bounce back, to recover from the nearly inevitable attack or mistake.

**Inside the company**

Any organization’s approach to cyber risk management should focus on people, process and technology, says Zurich’s Tim Stapleton. Some experts contend, he adds, that 90 percent of breaches could be avoided by following security basics.

**As always, it comes down to people**

Winning hearts and minds is critical to mitigating cyber risk. And in this sense, making progress in cyber security is no different to any other corporate challenge. First, somebody must be held accountable. Second, awareness and best practices need to be widely circulated throughout the organization.

**Accountability**

Who better to coordinate this than the corporate risk manager? According to several U.S. and European organizations have assembled data-security committees from a cross section of the organization, including the risk management department. “The risk manager is often viewed as the conduit to a holistic risk management approach to security and privacy risk across all areas of an organization,” explains Zurich’s Lori Bailey.

This can run contrary to traditional practice, which often sees cyber risk as a job for the IT department. A growing number of organizations are now realizing that cyber security extends well beyond the IT department. A wide range of issues such as lost or stolen data, violation of privacy laws, intellectual property infringement and social media-related risks such as cyber bullying and textual harassment constitute a much broader scope of cyber exposures.

A number of companies are going even further by appointing a Chief Information Security Officer (CSIO). Doing so lowers a firm’s data-breach costs.

**Cyber-safe processes**

Once accountability is defined, ‘cyber-safe’ practices need to be built into a company’s business processes. Core activities here, says Zurich’s Tim Stapleton, are to:

- Implement processes and procedures, such as security for physical records, restrictions on using mobile media and personal devices in the workplace.
- Ensure cross-functional, enterprise-level understanding of the risks so that technology, human resources and marketing departments collaborate, share and coordinate activities.
- Ensure third-party providers, such as outsource providers handling sensitive information meet your data-security protocols.

For instance, what about social media? Companies should think through their approach to Facebook®, LinkedIn®, Twitter® and the like. Approaches toward their use will range from prohibition to encouragement – the point is to have a clear policy. Many organizations still do not. A survey commissioned by Zurich showed that about three out of four companies have one clear policy, on average.\(^{30}\)

Another key aspect is simply to define the ‘crown jewels’ of a company’s data. Whether these are customer details, credit card data, intellectual property or knowledge, there should be a clear understanding what value they bring to the organization, says

---


"Complete prevention may be impossible. Planning can make all the difference to response and recovery."
the Institute of Risk Management in its report ‘Cyber Risk.’ Nearly all data breaches involve relatively simple techniques. A study by the UK government noted that ‘basic information risk management’ and security controls would probably defeat 80 percent of cyber attacks.

Technical defences
Naturally there are technical barriers that can and should be put in the way of accident and attack. Indeed, Zurich is cooperating with the digital security company Kudelski Group to offer cutting-edge tools (see box). This includes authentication, cryptography, intrusion detection/prevention systems, secure application development, virtual private networks and virus protection and Patch Management.

For the non-technical reader of this paper, the key point to remember is that technology is only one piece of the security puzzle. By themselves, clever software and hardware cannot ensure information security.

Resilience and insurance
To mount the best defence against cyber risk, experience suggests that it is not enough to task the right people, make processes safe and build the right firewalls. On top of this, you need to be prepared to come back from the inevitable accident or attack. Insurance can cover not just the losses, but the costs of this comeback.

Preparing for the breach
The sad fact is that some kind of breach, somewhere, somehow is almost inevitable. So while having people and processes sorted will dampen frequency and magnitude, it will still be necessary to have a recovery plan.

For its corporate customers, Zurich helps address this in three main parts.

- Getting ready: Do you have a response team in place? How will you know when you’ve been breached? Do you conduct audits of data collection activities, including third-party and cloud service providers? Where is sensitive information held and stored, and is it secure? Do you have audited data flows across your company and vendors, including a privacy and security review? Are employees adequately trained and prepared to notify cases of data loss or attacks? Are you aware of the regulatory requirements? Do you have access to specialist service providers, such as public relations and risk management? How do you communicate to customers, partners and stockholders once an incident has occurred?
- The fire drill: Do you know how to perform a forensic examination to determine how many records have been affected? Who needs to be informed within the organization?

The Kudelski-Zurich team
In late 2013, Zurich announced that it would cooperate with Kudelski Security, the cyber security division of Kudelski Group, in supporting an innovative cyber insurance product.

Kudelski Security combines more than 20 years of technological know-how with legal expertise, compliance, field investigation and crisis communication, according to Christophe Nicolas, a senior vice president at Kudelski Security.

“We are honoured to team up with Zurich to offer its clients a new range of solutions such as cyber risk assessments and consulting, as well as an alert response team,” he said.

and who can help? How can damage be contained? When should victims be notified and how much should they be told? Should you set up a call centre to help victims? What credit/identity monitoring and fraud remediation services must be provided? How do you restore your reputation in the marketplace? How will you defend yourself in court or against regulators?

- The aftermath: Following up on the fire drill, you need to establish what costs are covered by insurance and what budget covers additional spending, investigating the incident so as to learn lessons.

### Insurance

Companies should consider insurance for situations where their business falls victim to cyber predators or accidents. Some cover will be provided under conventional policies, yet more and more companies are finding that they also need additional, cyber-specific cover as well. In the U.S., for instance, 52 percent of some 300 companies surveyed on behalf of Zurich in 2013 reported buying cyber-liability insurance. This was up from 44 percent in 2012 and 35 percent in 2011.\(^{34}\)

#### Conventional coverage

Damages from cyber crime or cyber accidents will, to some extent, be covered under conventional insurance. A standard business liability policy, will cover ordinary losses such as damaged facilities, broken equipment, or ruined inventory. “Conventional coverage might include loss of electronic data as a result of equipment failure or force majeure, but it most likely will not include some of the newer threats of the internet era,” according to consultancy Prism Risk Management.\(^ {35}\)

#### Cyber coverage

Zurich has worked to develop a Zurich Security and Privacy Protection Policy that covers those areas that conventional policies miss, and that also funds resilience. This consists of liability and first party cover, including privacy breach costs and business interruption, which can help mitigate negative publicity and customer dissatisfaction:

- Privacy-breach costs including: forensic investigation expenses of a company's computer system to determine the cause or extent of a privacy breach; and certain legal and public relations expenses.
- Digital asset replacement expense coverage.
- Business income loss and dependent business income loss coverage.
- Cyber extortion threat and reward payments coverage.

Third-party coverage includes limited coverage for regulatory proceedings defence costs and optional Internet media liability coverage:

- Security and privacy liability coverage, which includes coverage for regulatory proceedings defence costs.
- Civil fines and penalties coverage (available as an option).
- Internet media liability coverage (available as an option).

### Outside the company

Externally, it might pay for companies to become involved in the debate about public policy regarding cyber risk. This can be divided into two main areas: codes and standards; and legislation or regulation. Broadly speaking, the former can be seen as ‘carrots’ to encourage good behaviour, the latter as ‘sticks’ to discourage bad behaviour.

---


**Codes/standards**

The International Standards Organization (ISO) has an ISO 27000 family of standards to help organizations keep information assets secure. Companies can apply the standards, apply for certification and contribute to the further development of the standards. Zurich has already applied ISO 27000 to its underwriting of retail insurance, specifically to the Payment Card Industry Data Security Standard (PCI DSS).

The National Institute of Standards and Technology, part of the U.S. Department of Commerce, has a computer security division that researches cyber risk and also develops standards.

Numerous other initiatives – public, private and public-private cooperations – are underway in various regions and business sectors.

---

**Legislation/regulations**

With the rise of the Internet, and not least the emergence of WikiLeaks and the unfolding of the Edward Snowden affair, privacy has become a major public issue. Many countries now have so-called ‘data breach and privacy’ laws, which penalize companies for leaking secrets. Just one example is Hong Kong’s Personal Data (Privacy) Ordinance. Implemented in late 2012, the law imposes notification and consent requirements for data users, and enables fines and potentially significant criminal penalties for data users that violate these requirements.

Companies are advised to learn the rules of data privacy for their operating jurisdictions, and to take appropriate measures to ensure compliance.

36 For more information, see: http://www.27000.org/