Financial Institutions
Customer Industry Community

ZURICH

Tackling the growing risk of cyber crime

Discussion points for financial institutions

Contents

Tackling the growing risk of cyber crime

The risk of cyber attacks on financial institutions is highly topical but not a new issue. However, what is changing, and rapidly, is the scale, frequency and sophistication of attacks.

Welcome to the first of our financial institutions customer industry community white papers. The idea behind creating an informal community of our financial services sector customers, along with insurance and industry experts, is to enable us to share views on key risk management issues. That way, companies learn from the experiences of their peers and Zurich can act as a partner that promotes best practice approaches which benefit the whole community.

The risk of cyber attacks on financial institutions is highly topical but not a new issue. However, what is changing, and rapidly, is the scale, frequency and sophistication of attacks. Financial institutions rely on technology to deliver convenient internet services to customers and to operate more efficiently. But emerging threats and technology development, such as cloud computing, mean more action is needed to identify and mitigate the risks of cyber crime.

Cyber crime has become 'monetised', where illegally obtained data is bought and sold. As well as financial risk, reputations can be damaged and public confidence lost.

Discussions at a Zurich Risk Forum organised for the financial institutions customer industry community in October 2014 were based on the risk priorities identified by customers in a survey we commissioned. Perhaps unsurprisingly, cyber threat was high on that list. This white paper summarises the points that were debated during the Forum.

As well as white papers we will run webinars for financial institutions customer industry community members to gain insights and debate the issues you tell us are important.

If you would like further information about cyber risk, please contact:

Lori Bailey (lori.bailey@zurichna.com), Luca Ravazzolo (luca.ravazzolo@zurich.com) or Dominik Bark (dominik.bark@zurich.com).

And if you would like to know more about our financial institutions customer industry community, or to attend a webinar, please contact **Mirjam Buehlmann (mirjam.buehlmann@zurich.com).**

Lori Bailey
Global Head of Special Lines, Zurich General Insurance

Luca Ravazzolo
Global Financial Institutions Lead, Global Underwriting, Zurich General Insurance

Dominik Bark
Head of Financial Lines for Europe, Middle East and Africa (EMEA), Zurich Global Corporate

The scale of cyber risk

Cyber crime is a growing problem and financial institutions now rate it as the number-one risk they face.

When news hit the headlines that JP Morgan Chase had become one of the latest financial service casualties of a serious cyber attack, the general reaction appeared to suggest that such news is no longer shocking.

It also indicates that while financial institutions may recognise the scale of the problems they face, many are still some way from finding the best ways to manage and reduce risk from cyberspace.

JP Morgan Chase said that the accounts of 76 million households and seven million small businesses had been hacked, making it one of the largest cyber attacks of its kind discovered to date. According to reports, the attack had been under way for a month before it was discovered.

The Center for Strategic and International Studies points out that the returns from cyber crime are great and the risks are low for criminals. The Center estimates that the likely annual cost to the global economy from cyber crime is more than $400 billion*.

Increasing awareness

PwC's 2014 Global Economic Crime Survey** confirms the growing scale of cyber crime. According to the survey, one quarter of respondents said they had experienced a cyber crime and about one in 10 said they had suffered financial losses of more than $1 million. More financial services sector organisations (45%) had suffered an economic cyber crime compared with all other industries (34%).

PwC noted: "The key message from our survey results is this: while the financial services sector may be ahead of many industries in terms of prevention and detection of economic crime, more can and should be done by financial service organisations."

Changing attitudes to risk

Fines and penalties for cyber breaches can have a significant impact on reputations and public trust for financial institutions. Financial service organisations that responded to the PwC survey said what many feared most was the fallout from being caught up in money laundering. Almost one third said the most severe impact was reputational. Zurich's own research (see below) confirms this is the number-one risk in the financial services sector.

Yet PwC's survey found that around one quarter of financial services organisations did not conduct annual fraud risk assessments. Over half of those that had not conducted an audit during the survey period from August 2013 to February 2014 were unaware of how to carry out an audit or failed to see its value.

Troels Oerting, Head of the European Cybercrime Centre, in an interview with Computer Weekly magazine in October 2014, said losses due to fraud or crime can total €9 million in some months and much goes unreported. A proposed European Union directive on network and information security aims to make it compulsory for companies at a certain level to report security breaches.

*In its latest report, The US Secret Service Investigative Division***, reports that it helped to prevent over $1 billion in fraud losses from cybercrime in 2013, but acknowledged that it is up against skilled and organised crime networks.*

At the Zurich Risk Forum, Massimo Cotrozzi, Assistant Director – Fraud investigation & Dispute resolution, E&Y, said monetisation of computer hacking and the scale of problem make it a challenge for risk managers in financial institutions. The last 10 years have seen major changes in the way financial institutions are attacked. According to Massimo Cotrozzi,

"Three quarters of attacks are on applications, denial of service and card skimming."

Attitudes among financial service institutions are changing. Ernst & Young noted that 2013 was the first time that internal discoveries outnumbered external detection, which suggests companies are acting themselves to do something about the problem. This is supported by attitudes among financial service sector risk managers in Zurich's survey.

Zurich survey results

The survey undertaken by **Strategic Risk** magazine for Zurich asked its financial services customers to identify their top risk concerns. The threat of cyber crime was second only to regulatory requirements.

The top five risks

Cyber risks are both an emerged risk for which cover is available, and an emerging risk, where the insurance industry is still to develop comprehensive cover. For example, 'bring your own device', 'the internet of things' and cloud computing, present challenges for underwriters to identify the nature and scale of cyber risk.

The Zurich survey found that although risk management practices had, in general, improved, they had yet to reach the point where risk managers felt best practice was fully embedded in the culture of their organisations. The survey showed that this rated 5.7 out of 10, which indicates that there is significant room for improvement.

How well do you believe your company embeds a risk management culture?

The survey findings suggest that most risk management practices are driven by ***compliance and regulatory requirements****. They are regarded as a 'must-do' action and so may not be undertaken as comprehensively as they need to be.*

The survey showed that ***attitudes and cultural views need to shift so risk management is a 'want to do' activity****, bearing in mind the huge tangible and intangible costs that breaches in cyber security can cause.*

01

Do you believe risk management practices in the industry are improving?

An interesting point the survey raises is how organisations tackle the scale of cyber risk challenges. This involves a deeper understanding of cultural dimensions that have perhaps not been addressed yet. For example, to understand threats – both external and from employees –

Organisations need to combine elements of sociology, psychology and an understanding of human behaviour.

02

Has the economic crisis improved risk management's stature within the business?

Yes	No	No change
38%	14%	48%

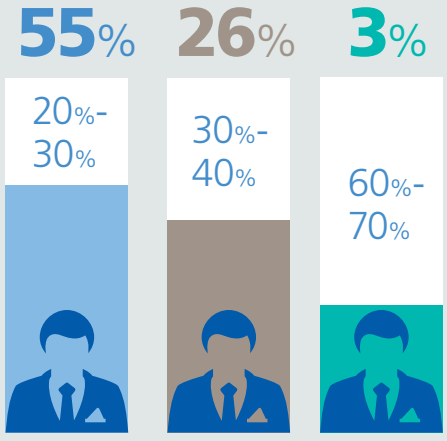
03

What are the hardest risks to insure?

It can be difficult to directly insure damage to reputation because once the damage is done, the company first needs to act quickly, mainly by ***taking immediate remediation*** *or mitigation actions or through specific communication campaigns. While several insurance products can provide cover for those actions and their related costs,* ***the main loss to the company resulting from the reputation damage can only be understood and addressed in the months following the damage****. This element will be hard to insure since it will be mostly deemed as business risk – for example, the loss of customers or costs required to address remedies or organisational changes.*

05

What percentage of your risks is insurable?



For 70% of a firm's exposures, most insurers have no solution.
Survey respondent

04

Understanding cyber threats

The Zurich Risk Forum highlighted how the nature of cyber attacks is changing. The challenge is compounded because cyber crime often crosses national borders and goes beyond attacks for financial gains to include political and activist – so-called hacktivist – activities.

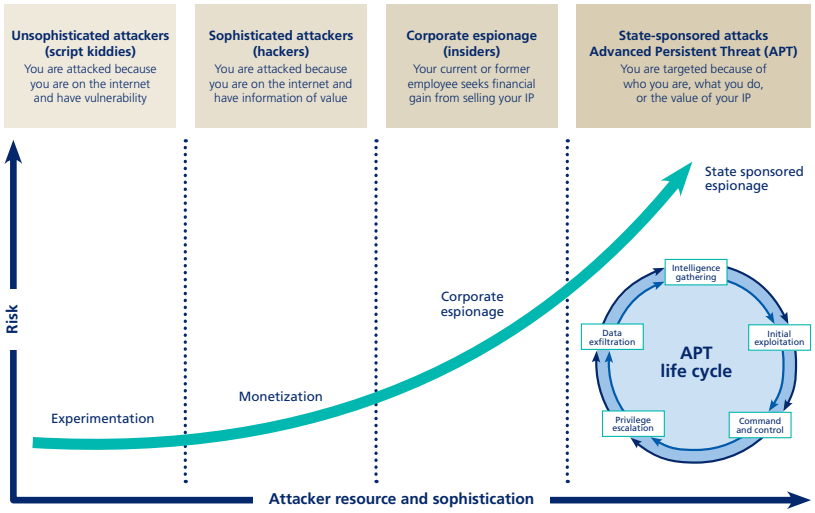
James Hatch, Director of Cyber Services, BAE Systems Applied Intelligence told the Zurich Risk Forum:

"We're talking about new tricks for old intents where financial institutions have to operate within the rules, whereas criminals do not. An over-reliance on older legacy systems in the financial services sector also has an impact on the ability to reduce risk."

Massimo Cotrozzi, Assistant Director – Fraud investigation & Dispute resolution, E&Y, pointed out at the Risk Forum that the issues affecting organisations around the world are not new. He said:

"What is changing is the pace of cyber attacks and the effects that they have."

Evolution of cyber threats



The story of computer hacking begins with individuals attempting to break into company computer systems simply to prove that it could be done – and that they were capable of outwitting security measures. The scale and rate of cyber attacks increased when the results of criminal activity gained a commercial value – for example, corporate espionage, stealing intellectual property or obtaining confidential customer information.

Cyber crime has developed into an 'on-demand' activity where information is bought and sold. Other types of attack are purely malicious – to destroy information or prevent an organisation from using its own computers – for example, through 'denial of service' attacks.

There are a number of characteristics of cyber threats that make them difficult to tackle. These include the following:

• Speed of attack

It can take minutes to compromise a system but days or even months to discover something is wrong. This period can give the hacker time to learn how the system works and they can possibly cause even more damage.

• Distance between attacker and victim

Cyberspace creates a distance between attacker and victim, making it hard to see the risks coming or to know how best to prevent them. The challenge of preventing cyber crime is made harder when crime crosses national borders. The perpetrators of computer crimes are often in different countries and different legal jurisdictions from the victims. Levels of multi-national co-operation are not always in place to deal with international criminal activities.

• Simultaneous, multiple attacks

Multiple attacks are often made on different organisations at the same time. This can create a sudden, massive problem that prolongs the period corporate computer systems are at risk, due to the length of time it takes to resolve the problems caused by the cyber attack.

Business activities that can increase cyber risks

Business activities can expose weaknesses in cyber protection. The following are times when organisations may be at their most vulnerable to attack:

• Mergers and acquisitions

When businesses merge, so do their IT systems. During a period when IT infrastructure is being upgraded and changed, organisations can be more vulnerable to attack. Cyber attacks can be external and internal – for example, from disgruntled employees.

• Entering new markets

Different markets may impose different regulatory conditions on cyber security that can impact the effectiveness of business operations and increase exposure to cyber risk.

• New product launches

Investment in research and development can be wasted if cyber criminals gain access to intellectual property or sensitive information. Data can be stolen or corrupted that could delay or damage commercial activities and damage brands and reputations.

• Major organisational change

Information security relies on robust mechanisms, a clear understanding by employees of how data security can be compromised, and a clear view of the risk landscape. Major organisational change can disrupt all of these.

• Target of activists

Big business is often included in protests against political and economic issues. Organisations in the spotlight can be at risk of attack, for example, from revenge-style attacks from disgruntled member of the public, customers or employees, as well as political protest and hacktivists seeking to make a point.

What should insurers be doing?

A panel debate at Zurich's Risk Forum highlighted the need for closer collaboration between insurers and their financial services sector customers.

For larger cyber risks, it was felt that insurers were beginning to realise that bespoke, rather than 'off-the-shelf' solutions, were necessary but more support from insurers was needed.

Bespoke solutions

The insurance industry must work harder to build cover around specific requirements – for example, with customised cyber, directors & officers and professional indemnity insurance products. Zurich confirmed it works closely with individual customers to develop tailored solutions appropriate to the cyber risks they face.

The challenge for insurance product innovation is that risks are evolving faster than the products. The insurance industry recognises this and is trying to broaden cover, for example, beyond financial losses by looking at operational aspects that can be affected by a cyber risk event.

Gaps in cover

The question arises of gaps in cover, where risk cannot be transferred to insurers. It was agreed at the Forum that this challenge was hard to address. Loss of reputation was an example. Delegates said they recognise the importance of shifting strategic thinking from risk prevention to threat detection.

Participants in the panel debate agreed that maintaining the confidentiality and integrity of data is an issue, as is ensuring the resilience of customer-critical systems. It was acknowledged that organisations need to have a far better understanding of who is attacking them, and why.

Developing solutions to cyber risks

Organisations need to prepare a cyber resilience and risk mitigation strategy from all angles. The Zurich Risk Forum highlighted a number of steps that can be taken to tackle cyber risk.

These include the following:

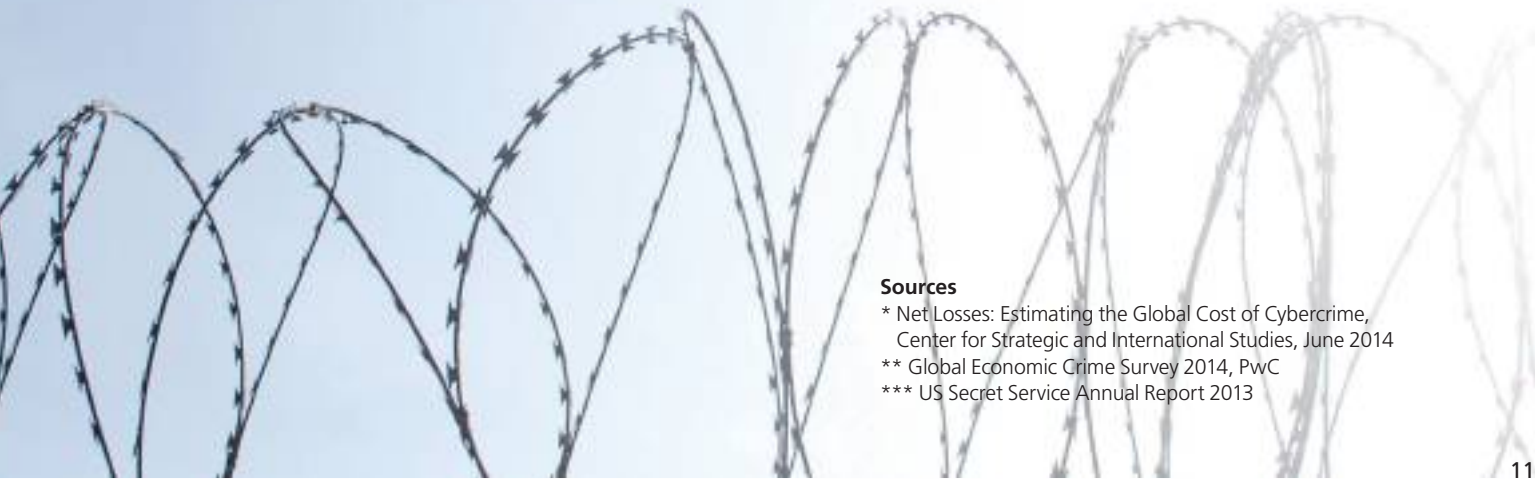
- Understand and prioritise the biggest risks, those that threaten reputation and front-line business assets.
- Plan for greater resilience to control and minimise the impact of cyber attacks.
- Understand who is targeting you.
- Gather threat intelligence.
- Monitor the effectiveness of cyber security monitoring.
- Identify vulnerabilities.
- Respond to incidents.
- Plan to rectify breaches in security.
- Set clear responsibilities for managing risk and ensure collaboration between departments – for example, risk managers and IT managers.

Taking an integrated approach

Ernst & Young recommends cyber risk solutions based on integrating security operations so businesses are able to align information security objectives with the changing threat landscape, their business goals and their appetite for risk. This can improve strategic decision-making that helps organisations to focus their investment and performance initiatives on areas where cyber risks are greatest.

Summary

- The scale and frequency of cyber attacks is increasing rapidly but understanding cyber risks lags behind.
- Cyber threats are one of the top risks identified by financial institutions.
- Businesses are more vulnerable at certain times – for example, during mergers and acquisitions and when they enter new markets.
- Financial institutions recognise many of the cyber risks they face and attitudes towards threats is changing, but more needs to be done to mitigate risk.
- Organisations should treat cyber security as a core part of their business activity by integrating risk management into their culture and making it a Board-level priority.
- Not all cyber risk is insurable, so prevention and risk mitigation planning is essential.
- Closer collaboration is needed between insurers and their financial institution customers to develop bespoke cover.
- Sharing information and best practice within the financial institution community can help in the development of robust insurance solutions.
- Solutions to cyber threats should focus on building resilience to mitigate risk. A good example is by taking an integrated, cross-functional approach to cyber security.



Sources

* Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies, June 2014

** Global Economic Crime Survey 2014, PwC

*** US Secret Service Annual Report 2013

www.zurich.com

138130A01 (11/14) ZCA

ZURICH®