KPMG

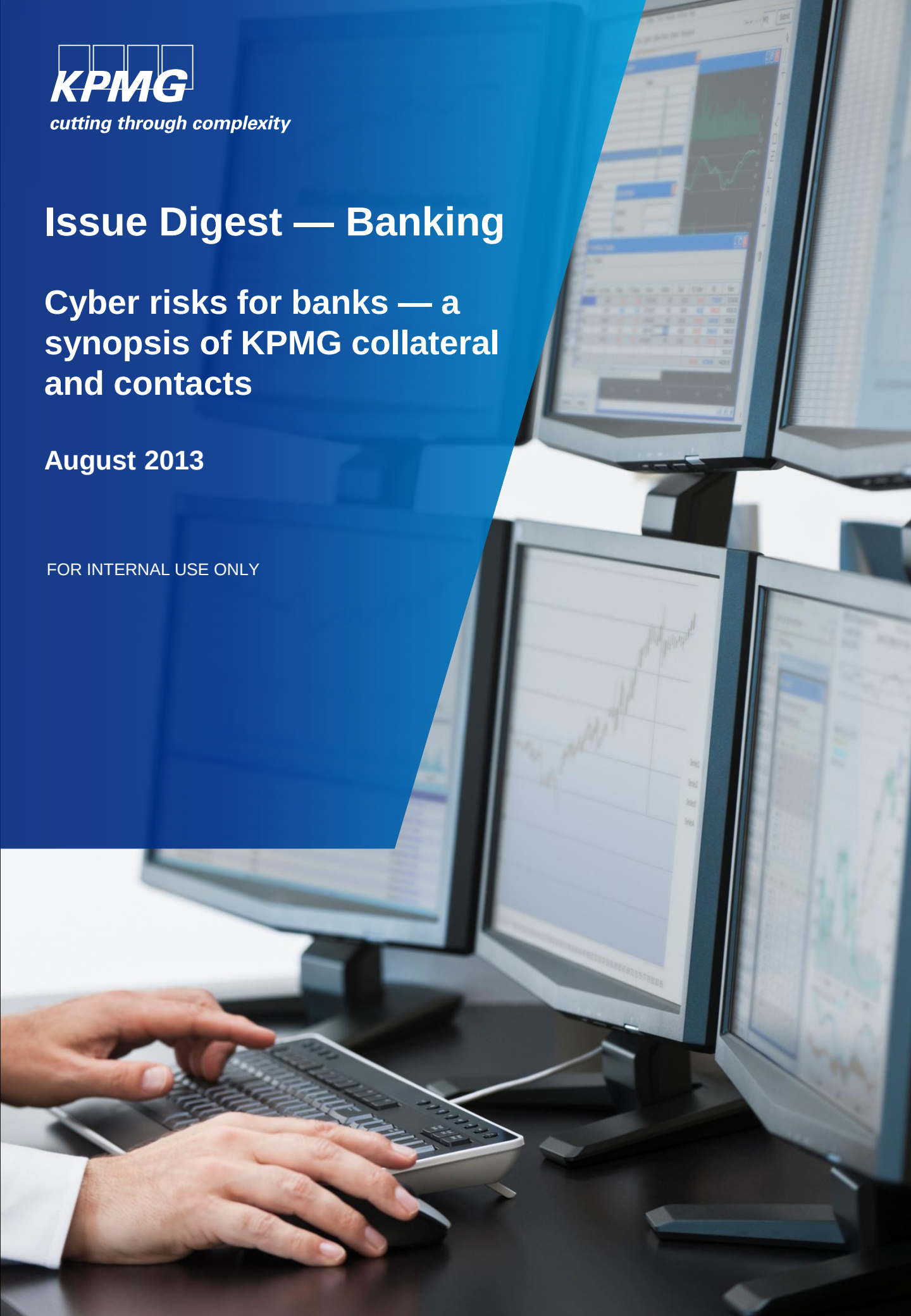
cutting through complexity

Issue Digest — Banking

Cyber risks for banks — a synopsis of KPMG collateral and contacts

August 2013

FOR INTERNAL USE ONLY



Content

Executive Summary

The classic image of a bank heist, replete with guns and balaclava-clad criminals, increasingly belongs in the past. Cyber crime, which is one of the fastest growing areas of crime is becoming a challenge to control. Some banks are considering cyber crime a threat to their stability and existence.

Increasing number of criminals are exploiting the speed, convenience and anonymity that modern technologies offer to commit a diverse range of criminal activities. The global nature of the internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace.

Digitization has made storage of data less costly and more efficient for banks; however, it has also increased the probability for data being stolen or getting corrupted.

Many organizations — banks, technology companies, consulting firms, cyber companies have been bringing this issue in the limelight. KPMG too has produced a number of internal and external documents on this critical topic. Through this report, we are making an attempt to bring forth a synopsis of our findings, the threats, and its impact on banks.

Digitization is increasing the threat and sophistication of cyber crime

The banking industry is one of the target industries for cyber criminals. According to Gordon Snow, Assistant Director of the Cyber Division of the Federal Bureau of Investigation (FBI), the frequency and sophistication of cyber crimes against banks is expected to rise further. Adoption of internet-based commerce systems provides more opportunities to steal information and hack systems. Some of the prominent reasons for cyber attacks are:

- **Toxic combinations**, which are created when individuals move positions but retain access to systems from their previous roles
- **Poor data management**, has made sensitive data vulnerable to cyber attacks
- **Digitization,** such as use of social media, mobile devices and remote access to network are increasing the probability of cyber security attacks
- **Lack of understanding by senior-level professionals** at banks and supervisory authorities about the extent of cyber threats and ways they can be tackled

Implications of rising cyber security threats for banks

Cyber security poses significant threat to the global financial institutions and the broader financial system. In the last few years, cyber threat frequency and sophistication has increased many folds. According to the research by Symantec Corp. (SYMC), cyber attacks have evolved from temporary website outages to robbing banks. Such threats can have following implications for banks:

- **Financial and reputational damage**: It increases the risk of loss of sensitive information (including intellectual property and trade secrets), which can result in financial (regulatory fines, compensation to victims of crime and theft of intellectual property) and reputational loss (loss of confidence in cyber transactions).
- **Systemic threat:** As banks and financial institutions are interconnected, an attack on one bank can leave other institutions vulnerable to disruption, threatening the security and stability of the broader financial system.
- **Increase in IT budget**: The heightened risk of cyber security attacks will result in banks increasing their IT budgets to enhance security measures such as antivirus software installation, incur cost of insurance and ensure IT security standards maintenance.
- **Disruption in business continuity**: A cyber attack can severely disrupt business operations, resulting in monetary losses.

Cyber security threats faced by the banking industry

Dealing with cyber security risks is a complex task. The current approach of banks' revolves around protection and compliance, as they are subject to increasing scrutiny from regulators and stakeholders. Therefore, there is a need to manage and protect information appropriately. Some of the leading cyber security threats for the banking industry identified by Federal Bureau of Investigation (FBI) are:

Key cyber security threats	Details	Example of breaches/damages
Account takeovers	Cyber criminals target personal computers of online banking customers via phishing e-mails or text messages to gain access to their accounts. Fraudulent money transfers and counterfeiting of stored value cards are the most common exploits of account takeovers.	FBI is investigating over 400 cases of corporate account takeovers. These cases involve attempted theft of over US$255 million and actual loss of approximately US$85 million.
Third-party payment processor breaches	Cyber criminals target computer networks of payment processors to hack personal data of customers.	Global Payments Inc., a payment processor was hit by a security breach in February 2012. The attack was estimated to have affected 1.5 million payment cards costing approximately US$94 million to settle fraud losses, fines and investigation costs.
Securities and market trading exploitation	Cyber criminals access brokerage accounts in a similar manner as they access bank accounts to conduct market manipulation and unauthorized stock trading.	A Russian national is facing charges of hacking into several online brokerage accounts in late 2010 to initiate fraudulent stock trades. Fidelity, Scottrade, E-Trade and Schwab have reported losses totalling approximately US$1 million as a consequence of the scam.
Mobile banking breaches	Cyber criminals gain access of user's credentials and account information by installing malware via a mobile application.	For example, cyber criminals have targeted mobile banking users by installing a variation of the Zeus malware via a website, text or mobile application.
ATM skimming	Cyber criminals fix a skimmer inside or outside the ATM to steal card number and personal identification number (PIN). They would then either sell the data or create fake cards to withdraw money.	Some of the common ways of conducting an ATM skimming are: 1) Attaching a card reader to the ATM to make a copy of the inserted card and 2) Installation of small cameras to record personal information.
Supply chain infiltration	Cyber criminals attack financial institutions suppliers of technology, software and hardware. Thus, when a financial institution installs the equipment or software impacted by a cyber crime it compromises its own security .	For example, ATMs supplied with malware installed or other defects comprising its security.

Way forward

Financial firms must be flexible and should develop technical sophistication to identify and tackle emerging cyber security threats. For this, senior-level management at banks supervisory authorities must have in-depth knowledge to clearly define and understand cyber risks. Currently, they have relatively limited understanding of cyber risks facing their firms. Further, experts believe banks lack a common framework to evaluate their cyber risk systems. Thus, banks need to develop a common framework with key risk and performance indicators to accurately understand the extent of cyber risk facing their firm.

Some of the takeaways and to dos for banks are:

- Build relationships for threat awareness with staff, executives, service providers, board of directors, customers, peers, professional organizations, law enforcement and regulators
- Follow regulatory guidance
- Perform ongoing risk assessments, including service providers for account takeover, DDoS (Distributed Denial of Service) and other threats
- Use layered controls for anomaly detection and monitoring
- Test capabilities and report to senior management and board

KPMG information, publications and contacts

Visit the following pages

External

Cyber security

Cyber response

Cyber vulnerability index

Internal

Information Protection and Business Resilience

Forensic technology services

Fraud risk management

Engagement credential

Cyber security thought leadership and related materials

Financial crime issue page

IT resilience client agenda

KPMG information, publications and contacts

KPMG publications and marketing collateral

Title	Project details
Reshaping banking in a dynamic business and regulatory climate	The report highlights some of the key issues that currently are shaping the industry. Some of issues emphasised in the report are technology, cyber security, big data, M&A, regulatory compliance and customers.
The cyber threat to your business	The paper showcases KPMG's understanding of cyber security and the approach it uses to understand the security system of an organization.
Cyber threat intelligence and the lessons from law	The report showcases KPMG's experience in information security law enforcement and experience of intelligence best practices along with the common pitfalls.
Information Privacy & Financial Institutions	Outlined in this paper is an overview of how information privacy changes the manner in which Financial Institutions process personal information. It highlights how the requirements will result in changes in the way employee and customer information is processed by a Financial Institution and its third parties.
Cybercrimes - A Financial Sector View	The paper is focussed on cyber crime issues, specifically in the financial services sector and the corresponding solutions to help tackle them.
Cyber Crime – A Growing Challenge for Governments	The report studies how cyber criminals continue to develop and advance their techniques and shift their targets — focusing less on theft of financial information and more on business espionage and accessing government information.
IT Advisory Services for banks and capital market firms	The paper addresses the needs of banks and capital market firms in regulatory compliance and IT risk management, information protection, governance, and third-party attestation.

Key contacts

Name of the contact	Designation	Country	Phone number
David DiCristofaro	Partner	United States	+0212 872 338
Gregory Bell	Partner	Canada	+1 613 212 2800
Stephen Bonner	Partner	United Kingdom	+44 20 76941644
Malcolm Marshall	Partner	United Kingdom	+44 20 73115456
Deborah Dacey LoPiccolo,	Director	United States	+1 201 505 3644
Mary A Mallery	Associate Director	United States	+1 201 505 3714
Irene Pitter	Sector Senior Manager, Global Banking	Germany	+49 40 32015 5322
Sarah Zahra	Marketing Senior Manager, Global Banking	Canada	+1 416 777 3468
Una O'Sullivan	Head of Knowledge Management, Global Financial Services	United Kingdom	+44 20 7311 1443

References

Banks Say Fed Should Lead in Cyber security for Industry

Major banks hit with biggest cyber attacks in history,money.cnn.com,September 2012

South Korean banks fall victim to biggest cyber attack in two years, livemint.com, March 2013

Cyber security essentials for banks and financial institutions, bankinfosecurity.com, 2012

The impact of cyber crime on business, Ponemon Institute, May 2012

New research reveals cyber security still not getting adequate attention from boards, emc.com, February 2012

Cyber security threats in financial services, boozallen.com, February 2012

FBI on Cyber security: Threats to the Financial Sector, September 2011

Global payments breach

Securities fraud hacker charged after $1 million heist, scmagazine.com, April 2012

Cyber security in financial institutions: a necessary framework for action, tapestrynetworks.com

Organized Cyber Crime and Bank Account Takeovers, March 2013

cutting through complexity