What Financial Institution Executives (and Boards) Should Know About Cyber Risk

QUANTIFY THE ENTERPRISE CONSEQUENCES OF CYBER RISK. CONTAIN EXPENDITURES COMMENSURATE WITH CORPORATE EXPOSURE

Today's cyber-powered Financial Systems present high-impact[1] risks to business and national interests. The increasing system complexity, exacerbated by high-speed trading, mark-to-market asset valuations and fluctuating money market rates, subject the entire financial system to exploitable vulnerabilities and systemic risks that – once triggered – may have runaway and severe financial, geopolitical and public confidence consequences. We can employ responsible IT hygiene and apply enterprise risk attention to avoid most significant consequences. However, we must adopt a new outlook – recognizing the new reality of a highly complex financial eco-system and adopting system engineering methods to understand and manage its behavior.

The new reality

This decade has seen everything about cyberspace change, except our ability to embody that change in our information management. Today's adversaries have worrisome motivations, significantly improved capabilities and are growing in number. They pursue financial, social and geopolitical agendas and are able to mount saturating numbers of attacks that defy attribution and response.

The Financial System has become a Complex Adaptive System-of-Systems. Andrew Haldane, Executive Director of the Bank of England, recently observed: "…systemic risk in the financial system is analogous to the reliability risks posed by complex networks encountered in fields such as ecology, epidemiology, biology and engineering…" As financial instruments, data (including Big Data), assets, organizations and technology become more complex, they become even more vulnerable to systemic failures, exploitable covert channels, operational instabilities, insertion of multiple simultaneous faults and more, and are exacerbated further by growing rosters of second-and-third-tier counterparties.

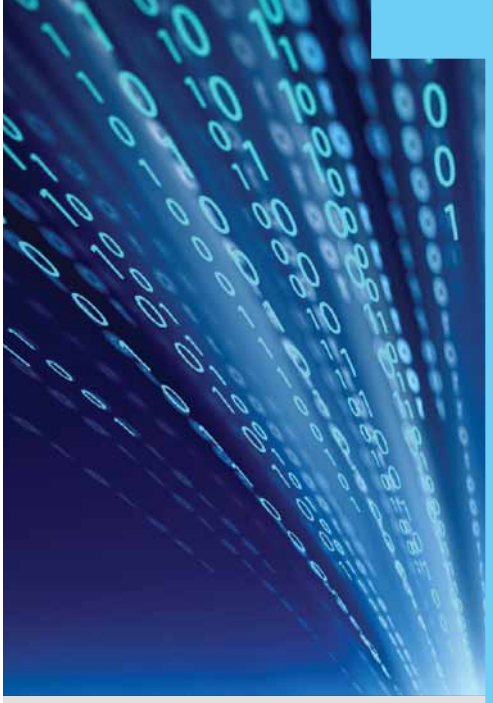
We are in a time of significant enterprise-level IT infrastructure change, including Cloud adoptions, M&A cyber integrations and mainframe-to-distributed processing conversions, which create transition situations, where company private and consumer personal information is exposed, compromising enterprise interests and raising regulatory (and legal) attention. In such transitional environments, information is often handled by third-party teams such as domestic or foreign outsourcers with temporary access, confused accountability and loosely-controlled test environments.

Most breaches can be managed, some still have enterprise impact

While cyber risk is a serious business and national concern, it need not be reason for panic or despair:

- Industry provides strong security technology and Government Agencies and NGOs (e.g. NIST, DHS, ANSI, and the Internet Security Alliance) provide very effective cyber security guidelines and best practices. Professional CISOs and their teams know how to apply them to modern IT systems.
- And corporate risk teams can identify and quantify those cyber consequences which do pose a 10Q (and concomitant share value) impact and then strengthen protections on high-impact Information Assets (with masking and obfuscation techniques, for example), and contain expenditures commensurate with exposure.

(1) "Almost 50% of Global 1000 companies lost 20% or more in share price in less than a month during the past 10 years - some never recovered. Most major losses were as a result of a series of high-impact but low-likelihood events…"
— Deloitte report, Disarming the Value Killers — A Risk Management Study



Adversaries & systemic Cyber Risks threaten the financial and public confidence interests of banks and governments

A recent Eurasia Group report opines that the impact of cyber attacks on the financial system "could be a long-term game changer for governments beyond the United States, corporations and banks, all of which are vulnerable to sudden, radical transparency."

Most breaches can be managed by diligent IT hygiene

Cyber Risk may still impact enterprise financial and brand interests

- Corporate officers must get in the game – to protect enterprise interests and to avert regulatory and legal over-reach.
- Quantify reportable financial and reputation exposure of YOUR cyber eco-system.
- Be mindful of M&A or Cloud cyber transitions and Legacy Systems where information assets are exposed under temporary, loosely-managed conditions

DataVantage®
Direct Computer Resources, Inc.

Beware of legacy systems and major transition programs which do not usually garner security attention and may be the source of hidden exposure and high exploitability

Cloud adoptions, M&A cyber integrations, mainframe-to-distributed processing conversions, even legacy system database upgrades all subject information assets to exposure from transition and/or testing circumstances. Often overlooked, this creates conditions where company sensitive and consumer private information (PII) may be compromised, raising additional regulatory (and legal) attention. In such environments, information is often handled by third-party (domestic and foreign) transition/test teams with loosely-controlled, albeit temporary, access and uncertain accountability.

- **M&A integrations** seek to realize significant cost savings by blending IT infrastructure along with operating and maintenance activities. They are motivated further by the desire to adopt common processes and procedures upon a freshly expanded client base. And, the need to consolidate financials and other inside corporate information drive plans to integrate merged information management systems. Here too, the end result poses no new security challenges but the transition presents exposures in porting, testing and commissioning the merged IT infrastructure with particular risk to information assets that affect stakeholder and regulatory interests. In M&A implementations, the database structures, schemas and applications are often from very different cyber environments and perhaps several generations apart and the implementation teams are sometimes comprised of unaccountable personnel handling information whose breach or exploitation invites legal and regulatory attention and potentially large financial losses.
- **Enterprises adopt the Cloud** to realize significant cost savings both in the ownership of data center assets and the labor associated with its operation and maintenance. Many companies are intimidated by its uncertain security and reliability, as IT space is shared with large numbers of anonymous users. Cloud-based operations may also seem to be out of your control. Actually, the Cloud is no more or less reliable than turning over IT infrastructure to third-party outsourced providers or even captive IT operations. It is little more than a modern high-speed version of "Time-sharing" from the 1970s and 1980s. Those systems had similar resource sharing and third-party control issues but users had little fear of security or reliability compromise. And the Federal Intelligence Community (IC) – such as the NSA and the CIA – both of whom know more about security than many – have already committed to moving 35% or more of their IT onto the Cloud. The real risk is not in the end result but in the transition. The porting of large databases from one implementation to another, the new groups of third parties managing the project, and the personnel and operating procedures for testing and verifying correct operation (often using "production" data), present uncertain situations where information may be leaked or altered, whether intentionally or inadvertently.
- **Legacy system changes,** from database system changes to complete mainframe-to-distributed system conversions subject information assets to users and test condition where accidental or malicious breaches exploit the casual security oversight that often prevails. Special care must be taken during testing for data accuracy, integrity and scalability. There may be considerable risk in using live production information (data), where new systems and personnel are involved who may expose vital information to breach or exploitation on a large scale.

WHAT CAN BE DONE?

A simple, inexpensive, four-part program can enhance an Enterprise Risk Management Plan by demonstrating due care and preventing significant financial, brand, regulatory and legal consequences:

1. Require your IT service providers (and counterparties) to adopt and maintain a program of cyber security education, best practices and compliance assurance. Whenever possible, use data privacy contractors whose products have been designated as anti-terrorism solutions by the DHS.
2. Maintain a prudent information sharing position with Federal and State Homeland security agencies that are able to provide timely threat data under the new Presidential Executive Order.
3. Establish and maintain an Enterprise Cyber Risk Balance Sheet to identify essential Business Confidential and Consumer Private Information Assets and quantify material financial and reputation breach consequences.
4. Protect those high-impact, enterprise vital Information Assets by protecting the underlying data – from the inside with DHS designated Anti-Terrorism Technology, combining encryption and supra-encryption techniques (such as masking and obfuscation) to insure privacy, protenction against reverse engineering and forensic hooks.

This requires corporate officers, indeed Boards, to get in the game – to be sure that enterprise risk components of cyber risk are considered – demonstrating due care, avoiding material, reportable consequences and averting legal or regulatory over-reach.

DataVantage®
Direct Computer Resources, Inc.

877.704.0077
www.DataVantage.com