NRI

Iakyara vol.232

Asset management companies' information security risks and defenses

Satoshi Idei

10.February.2016

Nomura Research Institute, Ltd.

Executive Summary

Some Japanese companies have recently incurred major losses from data leaks due to spear-phishing attacks or in-house criminal acts. With the Japanese government issuing new Cybersecurity Management Guidelines in December 2015, companies need to upgrade their information security, including asset management companies.

Satoshi Idei

Senior Technical Engineer

Asset Management Systems
Platform Services Department

Risks facing asset management companies

Information security risks, including spear-phishing attacks and criminal information leaks by insiders, are on the rise. For example, one study found that the financial services industry has a 5.6% customer churn rate attributable to data breaches[1]. At asset management companies, some IT staff apparently believe that their firms are less susceptible to information security breaches than large corporations. However, information theft (leak) incidents are not uncommon even among SMEs. According to an IPA[2] survey[3], 4.9% of Japanese SMEs have experienced theft/leaks customer information while 3.9% have experienced theft/leaks of confidential information about their own businesses. Another study found that half of all workers who have worked for more than one employer in their careers possess a former employer's confidential information and 40% of them kept the information with the intention of using it in their subsequent jobs[4]. Management must recognize that all businesses, not only major corporations, are exposed to information security risk.

What specific risks do asset management companies face? The IPA's Information Security Management Benchmark (ISM-Benchmark) service[5] has identified six metrics of structural susceptibility to information security risk. They are (1) permanent full-time employees' share of total workforce, (2) total number of business sites (both domestic and overseas), (3) degree of IT dependence, (4) degree of Internet dependence, (5) degree of dependence on business partners and (6) annualized employee turnover rate. I assume below that asset management companies' susceptibility to information security risk varies inversely with the first metric and directly with the other five metrics.

Asset management companies tend to have small, highly skilled workforces and therefore tend to be highly IT-dependent. Many asset management companies presumably store most of their confidential information on file servers. Absence of

NOTE

1) IBM, "2015 Cost of Data Breach Study: Global Analysis"

2) Information-technology Promotion Agency, Japan (www.ipa.go.jp)

3) https://www.ipa.go.jp/security/fy27/reports/cyber-ins/ (in Japanese)

4) Symantec, "What's Yours Is Mine: How Employees Are Putting Your Intellectual Property at Risk"

5) http://www.ipa.go.jp/security/english/benchmark_system.html

security measures such as file server access controls, access logs and safeguards against transferring company data from workplace computers to personal devices increases the risk of data leaks by non-regular or former employees or due to spear-phishing attacks.

Additionally, many asset management companies concentrate their workforces in core operations while outsourcing non-core operations, making them high dependent on external business partners such as printers, fund distributors, custodians, fund structurers, sponsors, rating agencies, information vendors and external asset managers acting as subadvisors. While many asset management companies are thus dependent on numerous external partners, the scale of their dealings with such partners are generally too small to justify building and maintaining dedicated IT systems or networks. Consequently, many asset management companies are presumably heavily dependent on the Internet (e.g., email, websites, FTP data exchanges) in their dealings with external partners. Without adequate security measures, these online communication technologies can easily be used to transfer important information by such means as uploading it to an external file sharing site or forwarding it as a file attachment to a personal email account. Moreover, asset management companies must be aware of the risk of their business partners being victimized by cyberattacks. The scope of the security risks facing asset management companies thus cannot be confined to the companies' own workforces or core IT systems. I encourage you to analyze and evaluate your own company's susceptibility to information security risk.

Security measures for asset management companies

To promote safeguards against such risks, Japan's regulatory authorities also have issued various guidelines. In April 2015, the Securities and Exchange Surveillance Commission (SESC) amended its Inspection Manual for Financial Instruments Business Operators[6] by expanding the scope of its inspections to include cyber-security. By so doing, the SESC aims to have investment trust management companies recognize cyber-security as a key management priority and adopt the following safeguards.

- Organizational measures (surveillance, reporting, public disclosure, CSIRT[7])
- Multilayered defenses (inbound measures, outbound measures, internal measures)
- Damage containment measures

6) http://www.fsa.go.jp/sesc/kensa/manual/kinyusyouhin.pdf (in Japanese)

7) CSIRT: computer security incident response team.

- Ongoing initiatives to address IT system weaknesses
- Periodic security evaluations and upgrades
- Adoption of authentication methods aligned with business operations and risks, and safeguards against employee misconduct
- Contingency planning, contingency plan training/updating and participation in industry-wide educational programs
- Training of cyber-security staff and formulation/implementation of cyber-security staffing plans

All of the above measures are intended to prevent or mitigate cyberattacks.

In December 2015, the Ministry of Economy, Trade and Industry (METI) issued Cybersecurity Management Guidelines[8]. The Guidelines require companies that utilize IT as an integral component of management strategy to comply with the following three principles as protection against cyberattacks.

- Management must identify cyber-security risks posed by IT utilization and play a leadership role in implementing safeguards against those risks.
- Management must implement security measures encompassing not only their own companies but also affiliated companies, supply chain constituents and any vendors to which IT system management has been outsourced.
- Management must communicate appropriately with stakeholders, including disclosure of information on cyber-security risks, security measures and incident responses during both exigent and normal times.

8) http://www.meti.go.jp/english/press/2015/1228_03.html

METI's Guidelines also set forth ten key matters[9] on which management should provide guidance to personnel in charge of information security (e.g., CISOs[10]). The Guidelines' appendices include specific checklists, recommendations on technological security measures and information on the Guidelines' relationship with international standards[11]. METI wants companies to incorporate the appendices' recommendations into their security measures. In the future, companies may be required to disclose information in accord with international standards and/or obtain certification of compliance with international standards.

9) The 10 key matters most notably include (1) leadership communication/structure, (2) cyber-security risk management framework, (3) risk-tailored safeguards against attacks and (4) preparedness in the event of a cyberattack.

10) CISO: chief information security officer.

11) Appendix C explains the relationship between the Guidelines and the ISO/IEC 27001/27002 international standards on information security management.

Information security going forward

Amid intensive IT utilization leading up to the 2020 Tokyo Olympics, IT talent shortages and information security measures will presumably broaden in scope. According to an IPA report[12], companies with 100 or more employees in Japan employ roughly 230,000 technology professionals in information security jobs, an estimated 22,000 fewer than actual demand for such personnel. Moreover, around 140,000 of these

12) http://www.ipa.go.jp/security/fy23/reports/jinzai/ (in Japanese)

230,000 personnel require some sort of additional education or training. In such an environment, asset management companies face difficulty recruiting and retaining qualified information security personnel.

Recently, information security services are increasingly becoming available from specialized third-party vendors, including diagnostic services, assistance with implementing information security regimes, security log analytics, and low-cost cloud-enabled security solutions[13]. However, even such external resources will likely soon be overwhelmed by demand. We urge asset management companies' top management to spearhead initiatives to upgrade and maintain their information security regimes without delay.

13) The NRI Group's product/service offerings include CIO/CSIRT support; assistance with security policy formulation; formation, operation and evaluation of internal CSIRTs; assistance with security troubleshooting, design and development; spear-phishing damage simulations; assistance with security incident response; terminal security; HR training; log monitoring service; prevention of mis-sent emails; email filtering; and private clouds (http://www.nri-secure.com/).

about NRI

Nomura Research Institute, Ltd. ("NRI", TYO: 4307) is an independent, global IT solutions and consulting services provider with annual sales of 406.0 billion yen as of FY ended March 2015. With front-to-back support for the buy- and sell-side, NRI's tradition of innovation has positioned them as a trusted international market leader. Leveraging NRI's global consulting business, NRI is able to provide innovative financial IT solutions for investment banks, asset managers, banks and insurance providers. For more information, visit www.nri.com.

Inquiries to : Financial IT Marketing Department
Nomura Research Institute, Ltd.
Marunouchi Kitaguchi Bldg.
1-6-5 Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan
E-mail : kyara@nri.co.jp

http://www.nri.com/global/opinion/lakyara/index