Featured Articles I

Financial Industry Examples

Incident Response Team Activities in Finance

Mari Miyazaki
Hiroyuki Hatanaka
Katsunori Takahashi
Momoko Nagata

OVERVIEW: With DDoS attacks and the spread of malware infiltration targeting Internet banking, there is a growing threat of cyber-attacks in the financial industry, one of the country's key infrastructure sectors. Against this background, financial institutions have responded by working rapidly to establish response measures for cyber-attacks, and are increasingly sharing cyber-attack-related information among themselves. Hitachi has a Group-wide incident response team called HIRT, with a financial sector subset called HIRT-FIS that promotes incident readiness activities for the financial sector. Hitachi also operates a joint internet banking center, which has continually provided security measures to combat today's constantly changing threats since the service started.

INTRODUCTION

SOFTWARE vulnerabilities, security incidents, and security accidents are being reported on a daily basis and represent major threats not only to key infrastructure companies, but also to the organizations in charge of the systems of those companies. Hitachi, Ltd.'s Financial Information Systems Division has helped create safe and secure financial systems through activities such as revising the Security Guidelines on Computer Systems for Banking and Related Financial Institutions (hereafter, FISC Security Guidelines) published by the Center for Financial Industry Information Systems (FISC), and constructing and operating systems designed in conformance with these guidelines.

However, recently, the repeated occurrence of unauthorized funds transfers done through Internet banking using malware, and the increase in activities taking advantage of the dissemination of vulnerability intelligence are creating a demand for fresh approaches at financial sites. This article discusses Hitachi's work on security measures in the financial sector.

SECURITY TRENDS IN THE FINANCIAL INDUSTRY

Financial Services Agency Activities

In April 2015, Japan's Financial Services Agency (FSA) revised some of its guidelines relating to system risks and Internet banking such as its Comprehensive Guidelines for Supervision of Major Banks, etc. and its Financial Inspection Manual.

The revisions call strongly for ensuring the security of Internet banking, and for developing cybersecurity management measures such as Computer Security Incident Response Teams (CSIRTs). They also make reference to specific technical measures in the form of intrusion detection systems, distributed denial of service (DDoS) attack response measures, and detection/blocking of improper communication.

In July 2015, the FSA released its Policy Approaches to Strengthen Cyber Security in the Financial Sector. In line with these policies, hearings were conducted to determine the state of work on cybersecurity management measures at financial institutions, and the efficacy of these measures.

FISC Activities

In June 2013, FISC established the Council of Experts on Countermeasures Against Cyber Attacks on Financial Institutions. The council consisted of experts from industry and academia (with members from government taking part as observers). It investigated the current state of cyber-attacks on financial institutions along with future efforts, and ultimately created a report of its findings. The report was used to investigate revisions in the FISC Security Guidelines (Revised Supplement to the Eighth Edition)

published by FISC, to which new items pertaining to the establishment of cyber-attack response measures were added.

In July 2015, FISC started a new initiative, administering the FISC Cyber Security Reference Information. This initiative consists of releasing useful notes and reference information when an event such as a security incident occurs, to ensure that the FISC Security Guidelines are interpreted properly.

Information-sharing Community Activities

Recently, financial institutions have been increasingly coordinating their cyber-attack-related information by joining information-sharing communities.

The Financials Information Sharing and Analysis Center Japan (Financials ISAC Japan) organization was created for sharing cybersecurity-related information among Japanese financial institutions. It originated from security study groups from major financial institutions, and began operation in November 2014.

According to the Financials ISAC Japan website, the organization has a total of 222 members (full members and associate members) as of the end of April 2016. Financials ISAC Japan shares information on incidents and vulnerabilities, and organizes working group activities on individual topics related to specific key issues.

Financial institutions that have created in-house CSIRTs are joining the Nippon Computer Security Incident Response Team Association (NCA). The NCA is a community created in 2007 to enable information sharing and coordination among Japanese CSIRTs. As of April 2016, it has a total of 137 member teams, of which 27 are CSIRTs in financial institutions. Membership is expected to continue to grow in the future.

This is how the culture of sharing cybersecurity-related information is rapidly being formed among Japanese financial institutions.

SECURITY INITIATIVES IN INTERNET BANKING

Responding to Unauthorized Funds Transfer Losses

The situation surrounding Internet banking has changed dramatically over the past few years. Publicly-released materials from Japan's National Police Agency show that losses to Japanese financial institutions from unauthorized funds transfers have been rapidly increasing since about 2013, with the amount of losses surpassing 3 billion yen for the first time in 2015. There is no doubt that measures to combat losses from unauthorized funds transfers are currently considered the most crucial area of security measures among banks.

Since beginning operation in 1999, Hitachi's joint internet banking center has responded to a widely evolving array of cyber-attacks by continually providing security measures to combat these ever-changing threats. While it is difficult to predict unknown threats that could occur in the future and take action beforehand, effective security measures for threats that have been identified so far are scheduled for wholesale and retail release in FY2016. Through these releases, the joint internet banking center plans to complete its release of functions for security measures conforming to the Japanese Bankers Association's "Understanding" on Improving/Strengthening Security Measures released by the Japanese Bankers Association.

Hitachi's joint internet banking center also works on early detection and prevention of losses from unauthorized funds transfers through operations-based measures. If a depositor suffers a loss from an unauthorized transfer, the joint internet banking center investigates whether similar unauthorized funds transfer losses have occurred in the past at any other banks, and immediately contacts those banks if suspicious transactions are found. It also monitors account access in anticipation of similar unauthorized funds transfers occurring in the future. If a monitored account is accessed, the relevant institution is contacted immediately to enable early discovery.

FISC Compliance

To provide comprehensive security measures for Internet banking, Hitachi is working on facility-, operations-, and technology-based security measures in conformance with the FISC Security Guidelines.

In the area of equipment, it has created data center facilities that offer high reliability, safety, and confidentiality, and conform to official standards such as those set by the International Organization for Standardization (ISO) (see Fig. 1).

In the area of operations, Hitachi has created operations management standards, and uses internal and external audits to check the efficacy of management standards and investigate items for implementation.

In the area of technology, it is working to protect information resources and public servers connected to the Internet through multiple network- and application-level measures, and is investigating efficacy through periodic vulnerability checks.

Location/building

- Highly safe region and ground environment with few natural disasters
- The spread foundation structure employed can withstand earthquakes of up to magnitude 7 on the Japanese scale (as large as the 2011 Great East Japan Earthquake).
- Close to police stations/fire stations
- Equipment conforms to financial industry FISC standards

Power/air conditioning equipment

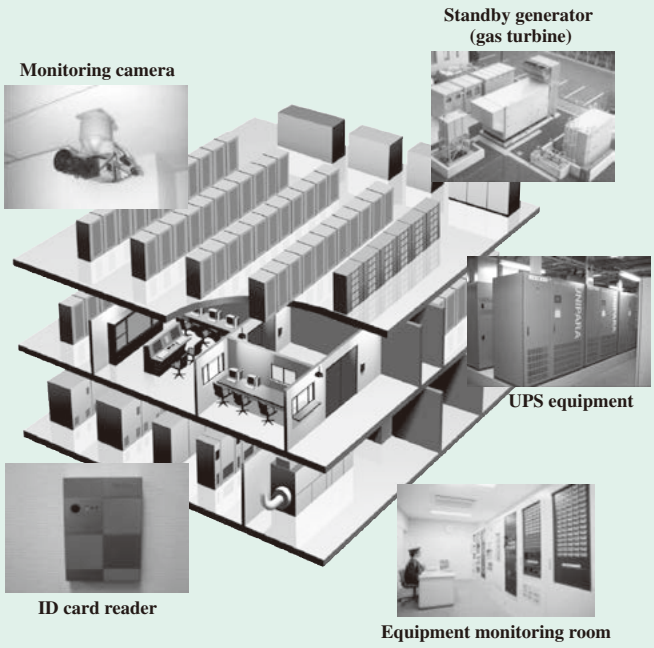
- Powered directly by underground cables from the power station
- Power equipment redundancy eliminates power failures.
- Equipment such as UPS and a standby generator ensure power failure readiness.
- The air-cooled air conditioning equipment shuts off the water supply during disasters.

Information security

- Security management conforming to ISMS certification standard
- Operation and management system conforming to ISO 9000 quality control systems

Other

- A hardware maintenance team is stationed in the same building.



FISC: Center for Financial Industry Information Systems UPS: uninterruptible power supply ISMS: information security management system
ISO: International Organization for Standardization ID: identification

Fig. 1—Data Center Equipment at Hitachi's Joint Internet Banking Center.
Data center equipment conforming to industry standards and official standards such as FISC standards, ISO 27001, and ISO 9000 enables high reliability, safety, and confidentiality.

CSIRT ACTIVITIES IN THE FINANCIAL SECTOR: HIRT-FIS

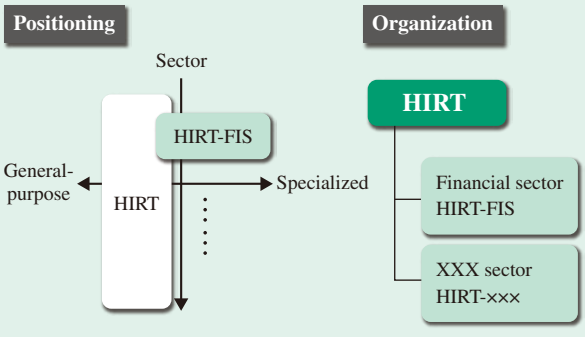
The Hitachi Incident Response Team (HIRT) is Hitachi's CSIRT. In October 2012, a subset of HIRT called Financial Industry Information Systems HIRT (HIRT-FIS) was created for the financial sector (see Fig. 2).

HIRT-FIS engages in incident readiness activities in the financial sector, aiming to serve as a professional CSIRT team specializing in the sector, while keeping abreast of industry-specific conditions and trends through FSA and FISC regulations and guides.

Activities within the Organization

To respond to cyber-attacks, it is vital to keep abreast of current threats and be quick to study and implement responses. HIRT-FIS makes daily checks of publicly-released incident information, and posts it on its intranet site.

The aim of these activities is to provide the latest security information to Hitachi sales representatives and system engineers (SEs) who are involved with the



HIRT: Hitachi Incident Response Team
HIRT-FIS: Financial Industry Information Systems HIRT

Fig. 2—HIRT-FIS Positioning.
HIRT-FIS is located within the Financial Information Systems Division, as the financial sector subset of HIRT.

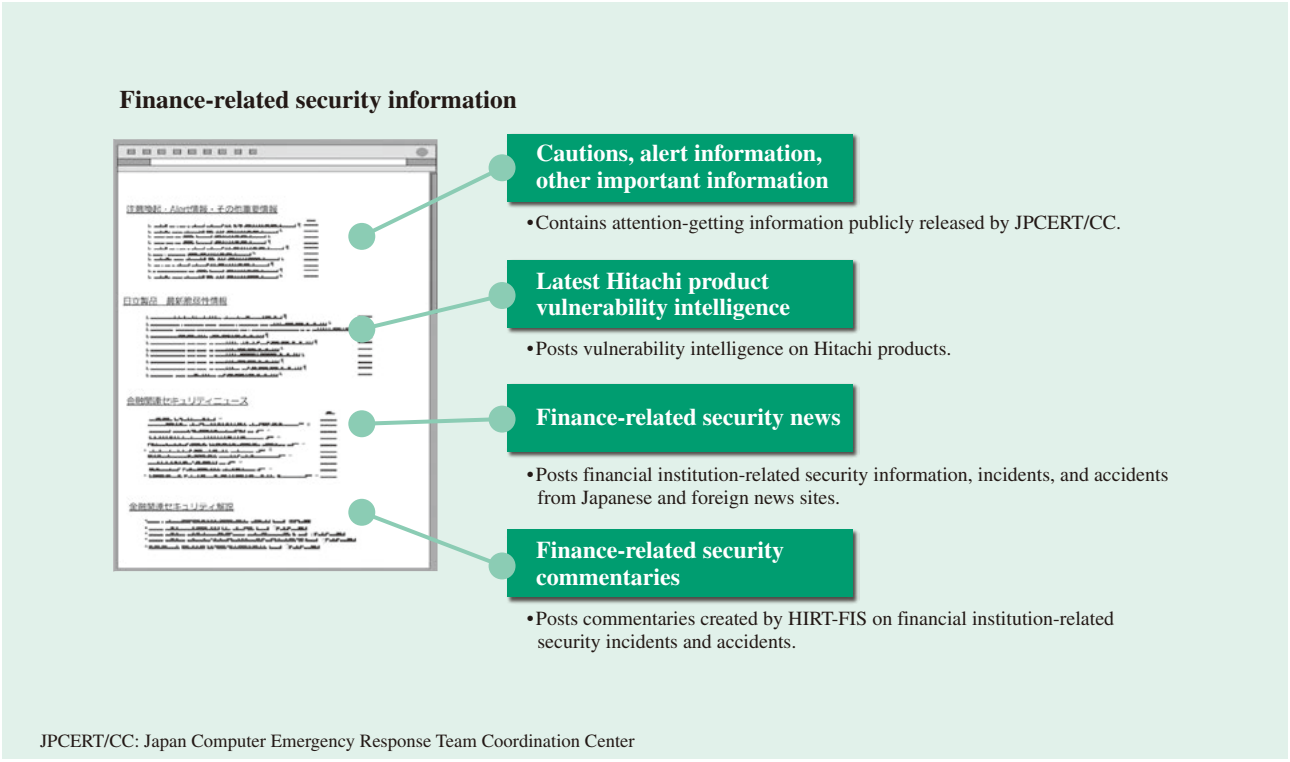


Fig. 3—HIRT-FIS Portal.
HIRT-FIS posts finance-related security information on its intranet site.

financial industry, to enable as early a start as possible for activities to reduce anticipated threats. Information is posted in the following four categories (see Fig. 3):
(1) Cautions, alert information, other important information

Mainly consists of alert information publicly released by the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

(2) Latest Hitachi product vulnerability intelligence

Consists of vulnerability intelligence publicly released by Hitachi.

(3) Finance-related security news

Consists of incident information related to financial institutions in Japan and abroad.

(4) Finance-related security commentaries

Consists of commentaries created on topics of high concern.

This information is used to help respond to inquiries received from other Hitachi departments, to assist with reviews of documentation such as security designs and security operation procedures, and to assist with evaluations of vulnerability check results.

HIRT-FIS is also responsible for creating security guides for SEs, disseminating information in-house through an email newsletter, and training financial sector security staff.

Coordination Activities among Organizations

HIRT acts as Hitachi's CSIRT office for dealing with external organizations, providing assistance with cybersecurity measures. It also works on improving CSIRT coordination among organizations through the NCA. This activity is designed to enable coordination among CSIRTs at different organizations, providing a more sweeping view of cyber-attacks for use in problem-solving, and enabling mutual assistance with activities.

As HIRT's financial subset, the role of HIRT-FIS in this activity is to coordinate financial institution CSIRTs.

CONCLUSIONS

This article has described the state of cybersecurity for financial systems, the security work being done by Hitachi's joint internet banking center, and the work being done by HIRT-FIS.

Financial institutions have traditionally changed staff roles through a rotation system, including staff who work with information systems. However, financial institutions are flexibly altering their human resources policies, making changes such as handling the highly specialized jobs done by security staff as

special appointments. These changes indicate that cybersecurity response measures are taking firm hold in the financial industry, and that the environment for coordination among highly specialized CSIRTs is becoming more active.

Initiatives related to the services Hitachi provides, and initiatives engaged in by specialist security departments are the two pillars of Hitachi's security activities, and Hitachi believes these activities will help ensure safe and secure financial systems in partnership with financial institutions.

REFERENCES

(1) The Center for Financial Industry Information Systems Website, https://www.fisc.or.jp in Japanese.
(2) Financial Services Agency Website, http://www.fsa.go.jp in Japanese.
(3) Financials ISAC Japan Website, http://www.f-isac.jp in Japanese.
(4) Nippon CSIRT Association Website, http://www.nca.gr.jp in Japanese.
(5) National Police Agency Website, https://www.npa.go.jp in Japanese.

ABOUT THE AUTHORS

Mari Miyazaki
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Financial Institutions Business Unit, Hitachi, Ltd. She is currently engaged in CSIRT activities as HIRT-FIS staff.

Hiroyuki Hatanaka
Planning Group, Financial Channel Solution Department 1, Financial Channel Solution Business Unit, Financial Channel Solutions & Payment Services Division, Financial Institutions Business Unit, Hitachi, Ltd. He is currently engaged in the planning of financial channel solutions.

Katsunori Takahashi
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Financial Institutions Business Unit, Hitachi, Ltd. He is currently engaged in CSIRT activities as HIRT-FIS staff.

Momoko Nagata
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Financial Institutions Business Unit, Hitachi, Ltd. She is currently engaged in CSIRT activities as HIRT-FIS staff.