Information Security
in the Financial Services Industry

We protect what matters.

Shred-it®

The average cost of a data breach is highest in the U.S. compared to all other countries in the world –

$7.35 million

an increase from $7.01 million the year before.[1]

Contents

Overview/Introduction of Information Security	**4**
Information Security and the Financial Services Industry	**6**
Did you know?	**7**
Examples of Financial Services Industry Security Breaches	**8**
What Documents to Shred?	**9**
What Puts a Financial Services Organization At Risk for a Data Breach?	**10**
Privacy Laws	**12**
Tips and Best Practices for Information Security	**14**

Overview/Introduction of Information Security

Data security has to be top-of-mind in the workplace today.

Companies have a 1 in 4 chance of experiencing a data breach[2], an incident that can prove to be very costly. Businesses can face enormous financial costs, downtime, damage to reputation and loss of customers. Individuals who have their confidential and personal information stolen may become victims of identity theft and other crimes. While the physical theft of data on paper or a mobile device is still a concern, cyber theft has become the fastest growing crime in the U.S. Because technology changes so quickly, the data security landscape remains a constantly moving target too.

What can make all the difference is comprehensive data security. Workplaces must have policies and procedures in place to ensure the security of all their information assets, from creation through handling and storage, to destruction.

Every day, nearly five million data records – or 58 records per second – are lost or stolen worldwide.[3]

67% of Chief Information Security Officers (CISO) said that their companies would likely fall victim to a cyber attack or data breach in 2018.[4]

Shred-it®

Information Security and the Financial Services Industry

As the trusted keepers of their customer's confidential financial information, financial services firms must ensure that protecting against confidential data theft and other data breaches is kept a priority. Though heavily-regulated, the financial services industry is targeted more than any other industry and breaches in this sector have actually tripled over the past five years.[5] With more and more businesses and individuals doing their banking, bill payments and shopping online, the risk is much higher than ever before.

Though money is the biggest motivator, information thieves are also after account numbers and other data as this information can be used to help criminals commit bank account fraud, identity theft, and other forms of crime. As a result, there has never been a better time for financial services firms to put a full range of information security safeguards in place.

Did you know?

42% of

FINANCIAL SERVICES FIRMS HAVE EXPERIENCED

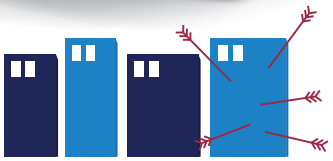
A DATA BREACH

The rate of data breaches in the last year has risen from 19% in 2016 to 24% in 2017.[6]

Financial services firms are the victims of almost **ONE QUARTER (24%) OF ALL DATA BREACHES.**[7]

CYBER ATTACKS

in the financial industry **COME FROM INSIDE THE BUSINESS.**[8]



The average financial services client organization experiences **65% MORE ATTACKS THAN ANY OTHER INDUSTRY.**[8]

ALMOST 90% of FINANCIAL IT PROFESSIONALS surveyed in 2017 said that their institution was **"VULNERABLE TO DATA THREATS".**[6]

FINANCIAL SERVICES FIRMS planned to spend more time and resources on **CYBER SECURITY IN 2017**[9]

FINANCIAL SERVICES FIRMS SAW AN INCREASE OF 389% IN THE NUMBER OF RECORDS STOLEN IN THE FIRST HALF OF 2017.[3]

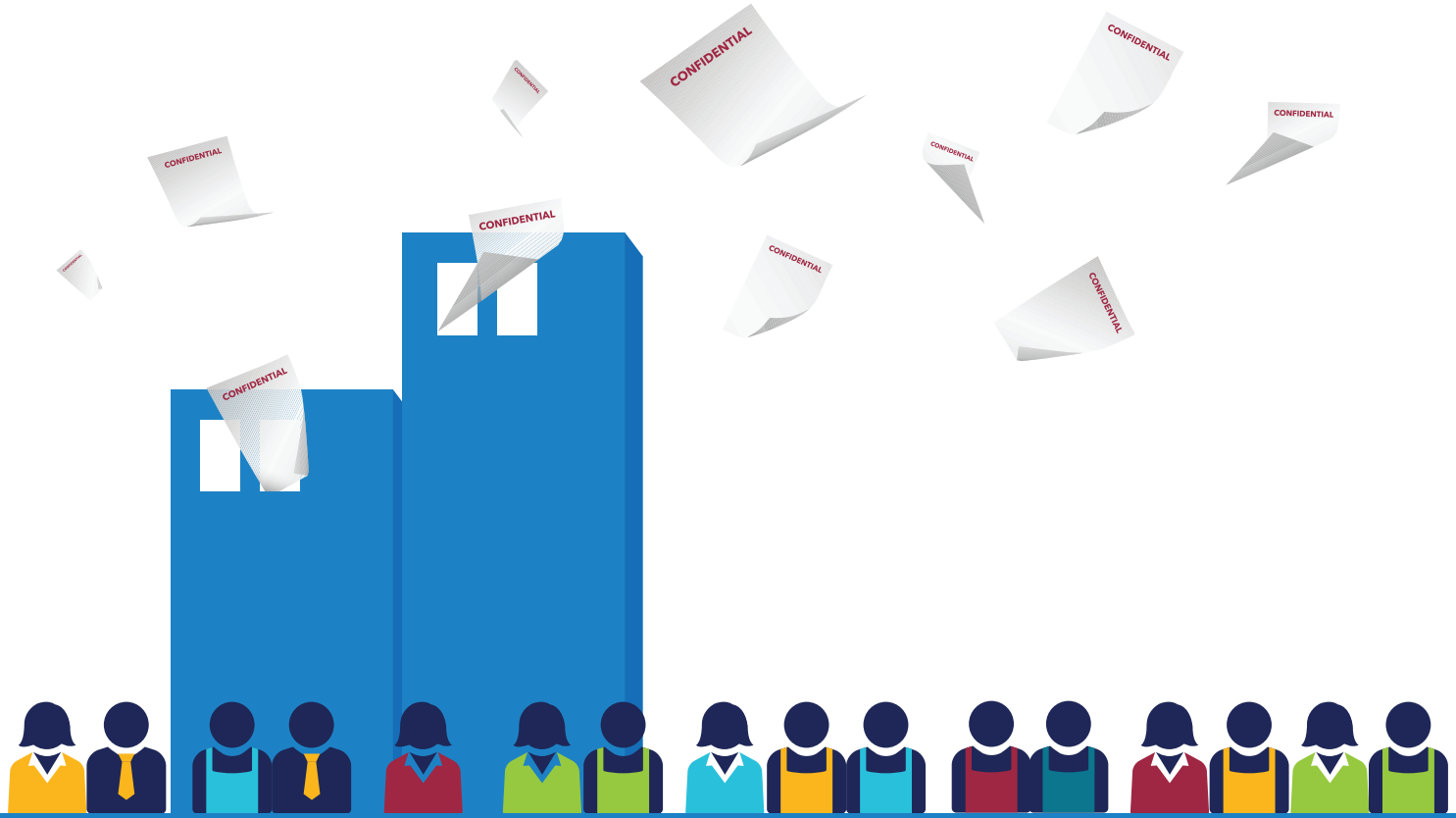
Shred-it®

Examples of Financial Services Industry Security Breaches

1. In 2017, cyber criminals hacked into one of the largest credit bureaus in the U.S. and stole the personal information of 147.9 million people. It is considered one of the worst breaches of all time because of the amount of sensitive information exposed, which included Social Security numbers, birth dates, addresses and drivers license numbers. The company revealed the hack two months after it happened, and said an application vulnerability on one of its websites led to the data breach. [11]

2. A man was caught on camera in 2017 allegedly stealing $17,000 from a credit union ATM. What is interesting was that Gainesville, Florida police said the suspect may have used login credentials from more than 40 people whose data was taken during an earlier restaurant data breach. That data was used to clone fake credit cards, which were then used with the PINs to withdraw the money from the ATM. The police believe the suspect may have bought the login information on the Dark Web.[12]

3. A financial services organization that specializes in the transfer of money across the world suffered a data breach early in 2018. The company, headquartered in Colorado, said that digital customer records had been accessed without authorization by cyber criminals at an external data storage company. When the breach was discovered, the company moved the records to another secure storage system and notified law enforcement.[13]



What Documents to Shred?

There are several documents used in the financial services industry that should be securely destroyed when no longer needed.

Customer Information

- Account numbers
- Personally Identifiable Information (PII)
- Loan applications and documentation
- Banking data

Accounting and Information Technology

- Customer lists
- Supplier information
- Internal reports
- Payroll statements

Human Resources

- Job applications
- Resumes
- Health and safety documentation
- Medical records
- Payroll information
- Performance appraisals
- Training information and manuals

Executive Level

- Budgets and other financial data
- Correspondence
- Legal contracts
- Strategic reports
- Financial statements

Shred-it®

What Puts a Financial Services Organization At Risk for a Data Breach?

Denial-of-Service (DoS) attacks:

DoS attacks {including distributed denial-of-service (DDoS) attacks and DoS botnet attacks} are the most common type of incident affecting the financial services industry.[7] They occur when cyber criminals flood a network or machine with traffic or send information to trigger a crash, resulting in loss of access to services.

Phishing scams:

A Business Email Compromise (BEC) scam is one of the most common scams used to try to trick victims out of money and confidential financial data. A criminal gains access to a corporate email account and spoofs the owner's identity to defraud the company.

Third-party partners:

Many financial service providers depend on multiple vendors, partners and other third parties to conduct business. But 60% of Chief Information Security Officers (CISOs) are concerned about a data breach from a compromised third party.[4]

Cyber criminals:

Cyber criminals (40%) are considered the biggest external threat to the financial services sector, followed by nation-states (18%), 'hacktivists' (16%), and business competitors (13%).[6]

Digitization:

Bank and other financial service providers are increasingly engaging with customers online, or via mobile phones and Internet of Things (IoT) devices, but various network connected devices are not always secure.

Insiders:

In a recent report, 60% of global financial services respondents cited privileged users as the biggest insider threat, followed by executive staff (48%) and contractors (38%).[6] Fraudulently transferring money or using personal information of customers for identity theft are examples of privilege misuse.

Dated equipment:

Financial services firms are constantly incorporating new technology, systems and software into their operations and legacy IT systems are often inherited from acquired organizations. Stockpiling these items can make the organization vulnerable to attack.

Negligent employees:

Research has shown that careless employees who don't follow proper policies and procedures are the biggest security threat in organizations.[16] Careless mistakes such as sharing passwords openly, carrying sensitive information unnecessarily and leaving mobile devices unattended outside of the workplace, can result in a data breach.

Financial malware:

With more than 1.2 million annual detections, financial malware is a huge threat and 2.5 times more common than ransomware.[14] In an earlier study, 75% of the top 20 U.S. commercial banks were infected with malware.[15]

Privacy Laws

The financial sector is heavily regulated and governed by privacy legislation at different government levels.

Here are several federal information security laws that apply:

Gramm-Leach-Bliley Act (GLB Act)

Requires financial institutions to explain information sharing practices to customers and to safeguard sensitive data. [17]

Fair Credit Reporting Act (FCRA)

Protects the privacy of consumer information contained in the files of consumer reporting agencies.[19]

Can-Spam Act

Sets rules for commercial email and requiring that emails are clearly identified as being from the financial institution.[25]

Fair and Accurate Credit Transactions Act (FACTA)

Helps reduce the risk of identity theft by regulating how consumer account information is handled.[23]

Payment Card Industry's Data Security Standard (PCI DSS)

Directs companies to protect cardholder data.[21]

Sarbanes-Oxley Act (SOX)

Helps protect investors from fraudulent accounting activities by corporations and includes financial disclosure requirements.[20]

Red Flags Rule

Requires the creation of an Identity Theft Prevention Program that detects the warning signs or 'red flags' of identity theft in day-to-day operations[18]

General Data Protection Regulation (GDPR)

Protects the personal data and privacy of citizens of the European Union (EU) and applies to all companies, anywhere in the world, that process any information about EU citizens. [22]

Disposal Rule

Part of FACTA, requires the proper disposal of information in consumer reports and records (paper must be immediately and securely shredded and/or the digital file is also destroyed).[24]

Personal Information Protection and Electronic Documents Act (PIPEDA)

Governs how private sector organizations in Canada collect, use and disclose personal information, and information must be protected by appropriate safeguards[26]


Reported cyber attacks against financial services firms rose by 80%
in the last year.[27]

Shred-it®

Tips and Best Practices for Information Security

Data security plan

Every financial services organization should have a comprehensive security program in place that covers people, policies and procedures. IT safeguards including spam filters, firewalls, encryption for all hard drives, DDoS detection software and data loss prevention (DLP) technology are critical.

Compliance and data privacy:

The financial services sector is heavily regulated and violations can be expensive and can destroy credibility. Conduct regular audits to ensure all regulations are being met. Compliance was the top reason for security spending at 49% of U.S. financial service respondents.[6]

Penetration testing:

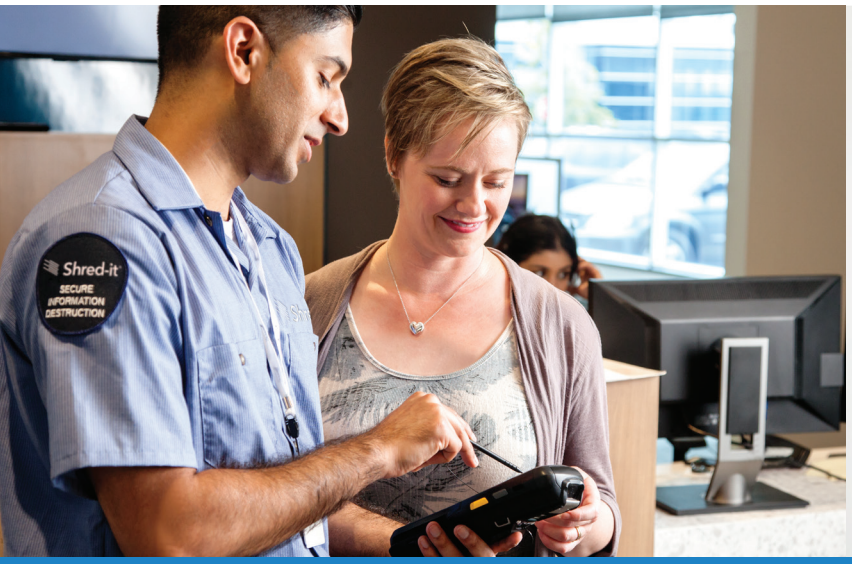
Conduct systems penetration and vulnerability testing to identify and fix security problems.

Culture of security:

Create a culture of security awareness throughout the organization. All employees, from executive level to front line, should demonstrate a commitment to information security.

Update software and hardware:

Conduct a regular check for patches or other updates to computer security software and operating system. Stay up-to-date with technology and securely destroy legacy equipment.



On-going employee training:

Educate all employees about data breaches and how they can help to avoid them.
Teach them how to identify dangerous threats, such as phishing scams.
Emphasize customer retention and activities to preserve reputation and brand value.
Training should be on-going especially because this sector has a 7.1% churn rate, the highest rate of all industry sectors.[1]

Password policy:

Enforce a password policy that requires strong passwords for each device, network, service and website. In a recent study, nearly three-quarters of financial services customers said they would use more than one password for authentication, and nearly 9 in 10 are open to using biometric security in the future.[10]

Third parties:

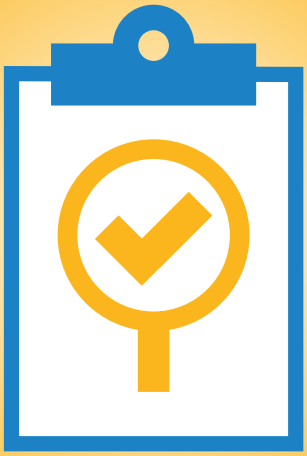
Choose third-parties with experience and commitment in data security.
They should be regulatory compliant too.

Disaster recovery:

Be prepared and have a breach response and disaster recovery plan in place.
Everyone should know what to do if a breach occurs.

Document destruction:

Partner with a document destruction company that has a secure chain of custody and provides destruction services for paper, hard drives and e-media.
A Certificate of Destruction should be issued after these items are destroyed.



Shred-it®

How Shred-it® Can Help

The Shred-it Protected Workplace

Our integrated suite of products and services - including Paper Shredding, Hard Drive Destruction and Workplace Security Policies, all delivered through a secure Chain of Custody – are designed to protect the things that matter most, every single day.

Shred-it Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody processes
- Certificate of Destruction after every service
- Tailored solutions to your organization's needs

Advice and Expertise

- Trained experts in information security
- Provide a Data Security Survey at your organization to identify information security risks

Learn more about information security in the financial services industry here: 888-227-0923 | shredit.com/finance

Sources:

1. 2017 Cost of Data Breach Study, United States, Ponemon Institute.
2. 2017 Cost of Data Breach Study, Global Overview, Ponemon Institute.
3. Breach Level Index, 2018, Gemalto.
4. What CISOs Worry About in 2018 Survey, 2017, Ponemon Institute and Opus.
5. 2017 Cost of Cyber Crime, Financial Services, Ponemon Institute and Accenture
6. 2017 Thales Data Threat Report, Financial Services Edition
7. 2017 Data Breach Investigations Report, 10th Edition, Verizon
8. IBM X-Force Threat Intelligence Index 2017
9. 86 Percent of Financial Services Firms to Increase Cyber Security Spend in 2017, eSecurityplanet.com, April, 2017
10. IBM Future of Identity Study, 2018.
11. The 17 Biggest Data Breaches of the 21st Century, CSOonline.com, January 2018.
12. Chipotle Data Breach Leads to Illegal ATM Withdrawal, Scmagazine.com, July 2017.
13. Western Union Customer Data Stolen, wccftech.com, February 2018.
14. Internet Security Threat Report, Financial Threats Review 2017, Symantec
15. 2016 Financial Industry Cybersecurity, Security ScoreCard
16. Promoting Data Security in the Workplace infographic, University of Alabama at Birmingham.; 2016 State of the Endpoint Report, Ponemon
17. Gramm-Leach-Bliley Act. Federal Trade Commission.
18. Red Flags Rule. Federal Trade Commission.
19. Fair Credit Reporting Act. Federal Trade Commission.
20. Sarbanes-Oxley Act. Soxlaw.com.
21. Payment Card Industry's Data Security Standard. Security Standards Council.
22. General Data Protection Regulation. Eugdpr.org.
23. Fair and Accurate Credit Transactions Act. Federal Trade Commission.
24. Disposal Rule. Federal Trade Commission.
25. Can-Spam Act. Federal Trade Commission.
26. Personal Information Protection and Electronic Documents Act. Office of the Privacy Commissioner of Canada.
27. Rise in Cyber Attacks Against Financial Services Firms, Information Age, January 2018.

Shred-it®