Information security — closing off access to sensitive data.

A white paper by

BACOMPT

The reality of cyberfraud.

"Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated," states the FBI.[1] "Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country."

According to a study conducted by the Ponemon Institute, "Heavily regulated industries such as healthcare, education, and financial organizations had a per capita data breach cost substantially above the overall mean."[2]

It can become a company's worst nightmare. Trade secrets, financial data, and health and other personal information are more vulnerable now than ever. And hackers just keep getting smarter, necessitating even the best network security measures ever-evolve just to keep up.

If it feels like you're treading quicksand, you're not alone.

The problem is so widespread that companies large and small are feeling the pressure — not only from their customers but the federal government as well — to ensure data safety.

In this white paper, we'll overview the federal mandates that are driving advancements in cybersecurity and the three pillars of data protection:

- Awareness training
- Vendor management
- Reporting

Table of contents.

"Today the message is loud and clear: HHS is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule..."

1. Federal Bureau of Investigation, https://www.fbi.gov/investigate/cyber. Accessed November 2017.

2. SecurityIntelligence, "2016 Ponemon Institute Cost of a Data Breach Study," https://securityintelligence.com/media/2016-cost-data-breach-study. Accessed November 2017.

Information Security — Federal Security Mandates

The escalating use of electronic documentation and sharing in the 1990s created heightened exposure and vulnerability not only for government, finance, and healthcare organizations, but also for their customers. This necessitated the enactment of federal laws mandating security standards.

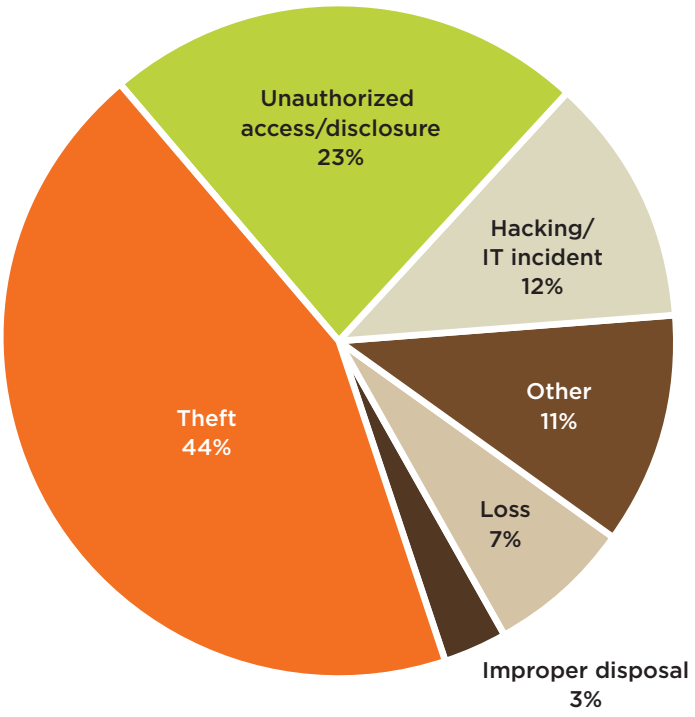
HIPAA.

The Health Insurance Portability and Accountability Act, or HIPAA, was signed into federal law in 1996. While Title I of HIPAA protects health insurance coverage for employees and their families who lose or change jobs, Title II requires strict adherence to national standards for the privacy, guardianship, and dissemination of electronic health records (EHR) that contain protected health information (PHI). In addition, Title II mandates the use of a national provider identifier (NPI) for every healthcare provider, including physicians, hospitals, and insurance companies.

If found in violation of HIPAA, healthcare organizations, as well as individual providers and employees, may face civil and/or criminal penalties. A striking example is the $4.3 million fine imposed by the US Department of Health and Human Services (HHS) in 2010 against Cignet Health for HIPAA Privacy Rule violations.[3]

"Today the message is loud and clear: HHS is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule and ensuring provider cooperation with our enforcement efforts," stated HHS' Office for Civil Rights Director Georgina Verdugo.[3]

HIPAA Privacy Violations by Type[4]



3. Health and Human Services, "Civil Money Penalty," http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health. Accessed November 2017.

4. Calyptix, "Discover the top 3 causes of HIPAA violations and their simple solutions," https://www.calyptix.com/hipaa/discover-the-top-3-causes-of-hipaa-violations-and-their-simple-solutions. Accessed November 2017.

GLBA.

The Gramm-Leach-Bliley Act, or GLBA, was proposed to remove barriers prohibiting different types of financial institutions (e.g., commercial banks, insurance companies, and securities companies) from consolidating. Because of concerns over the sharing of customers' personally identifiable information (PII) among a conglomerate's member companies, the final bill was signed into law in 1999 after provisions were made to strengthen privacy standards and enforce non-discriminatory economic opportunities.

GLBA contains the following three rules and provisions:

• **The financial privacy rule** requires financial institutions to inform their customers, via a privacy notice, what kinds of information they collect and with what types of businesses they intend to share this information. The privacy notice must also advise customers on how they can opt out of the disclosure.

• **The safeguard rule** requires all financial institutions and their affiliates to establish and maintain safeguards to protect PII.

• **Pretexting provisions** prohibit attaining PII through false pretenses; fraudulent statements; or forged, lost, or stolen documents.

The penalties for violating GLBA are punitive:[5]

• A financial institution can be fined up to $100,000 for each violation.
• Officers and directors can be fined up to $10,000 for each violation.
• Criminal penalties include imprisonment for up to five years, a fine, or both.
• If GLBA is violated at the same time that another federal law is violated, or if GLBA is violated as part of a pattern of any illegal activity involving more than $100,000 within a 12-month period, the violator's fine will be doubled, and he or she will be imprisoned for up to 10 years.

5. Ecora Software, "Practical Guide to Understanding and Complying with the Gramm-Leach-Bliley Act, www.ecora.com/Ecora/whitepapers/IDRS_GLBA.pdf. Accessed November 2017.

FISMA.

The Federal Information Security Management Act, or FISMA, addresses security interests of federal executive branch civilian agencies and requires each federal agency to adopt information security measures, including those that cover outside contractors. FISMA was signed into law in 2002 and applies to inventory and categorization of information, risk assessment, security controls and planning, accreditation, and monitoring.

According to the National Institute of Standards and Technology (NIST), "FISMA compliance requires the thoughtful selection and employment of stringent security controls for federal systems using a risk-based approach to protect critical federal missions and business functions. In addition to technology-based controls such as access control, identification and authentication, audit and accountability, encryption, and system and communications protection, there are also management and operational controls that address important security areas such as physical security, personnel security, continuity of operations, awareness and training, incident response, security planning, system integrity, and acquisition.[6]

"Developing sound security policies and procedures is a critical aspect of building an effective information security program. Security policies, while administrative in nature, demonstrate in clear and unequivocal teams, senior management's commitment to information security and protecting the organization's operations (mission, functions, image, and reputation) and assets, individuals, other organizations, and the nation… Effective policies and procedures, in conjunction with technology-based security controls, provide a defense-in-depth and holistic approach to information security and managing organizational risk from systems."[6]

The Federal Information Security Modernization Act of 2014 (FISMA 2014) amends FISMA by codifying the Department of Homeland Security's role in administering the implementation of information security policies for federal executive branch civilian agencies, overseeing agencies' compliance with those policies, and assisting the Office of Management and Budget in developing those policies.[7]

All federal agencies and all organizations working with a federal agency receive an annual compliance grade that is made public. A low grade may correspond to a greater vulnerability to a cyber-attack, resulting in job loss, potential hearings before Congress, and cancellation of funding for agency programs.

"Developing sound security policies and procedures is a critical aspect of building an effective information security program."

6. National Institute of Standards and Technology Computer Security Resource Center, https://csrc.nist.gov/projects/risk-management/faqs. Accessed November 2017.

7. Department of Homeland Security, https://www.dhs.gov/fisma. Accessed November 2017.

Prevention, detection, response, and reporting protocols are an absolute necessity in today's data-driven landscape. SecurityIntelligence, an IBM company, claims that spending on cyberinsurance has more than doubled to $2.5 billion in 2016 and estimates that global spending to combat cybercrime will top $80 billion this year. They also state that 62 percent of organizations use third-party managed security services as part of their cybercrime defense.[8] A summary of various information security tactics follows.

Awareness training.

The biggest threat to cybersecurity can be the unintentional actions of a company's own employees. This can occur when users inadvertently copy sensitive information to an internal public network folder or when personal files (containing customer names, Social Security numbers, and dates of birth) are accidentally copied into website forms. Yes, it happens. According to an ISACA conference survey, 21 percent of respondents report security breaches due to "non-malicious insiders," and only 58 percent of respondents mandate security awareness training for their employees.[9]

And this doesn't begin to account for the damage being done by malicious outsiders and malware.

It cannot be stressed enough that awareness training, at all levels from corporate management to IT and customer service, is the first critical step in mitigating risk. An effective awareness-training program should be developed from an annual acceptable use policy (AUP), which stipulates constraints and practices that a user must agree to for access to a corporate network or the internet. Implementation of AUP should include education, motivation, and activation and be measured through regular audits.

The education component is the "what" of awareness training: communicating the goals of the acceptable use policy. Motivation promotes the "why" of policies: access, passwords, even how customer service answers phone calls with offhand questions. Activation represents the "how" of awareness implementation: being on guard at all times. For instance, many clients — who are both educated and motivated — still fail simple social engineering tests, such as pretext calling and phishing, by being tricked into giving out sensitive information.

With rapidly evolving technology, as well as the rate of hacker sophistication, it's imperative to understand that awareness training is not a one-and-done. Ongoing training keeps all employees up to speed on current threats, as well as methods of response.

8. SecurityIntelligence, "20 Eye-Opening Cybercrime Statistics," https://securityintelligence.com/20-eye-opening-cybercrime-statistics. Accessed November 2017.

9. ISACA, "State of Cybersecurity Implications for 2016," https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf. Accessed November 2017.

Vendor management.

With the Target security breach in 2013, we're reminded that many incidents are caused not by primary providers, such as retail outlets and banks but, rather, by their vendors who handle sensitive information. These suppliers include, but are not limited to, data service providers, printers, and mailing companies.

Your company may have security protocols in place, but the essential question is how do your vendors (and their vendors) stack up? The supply chain is only as strong as its weakest link, and any contractor handling sensitive information should have the following security protocols in place:

• **Detailed risk assessment** provides proof through documentation that security protocols and infrastructure are in place and operating effectively. Risk assessments allow organizations to identify and adjust procedures and enable key staff members to collaborate and trouble-shoot from an attacker's perspective.

• **24/7/365 network monitoring** provides the ability to watch for negative traffic on the network, manage event logs, report changes to any critical asset (such as firewall), and provide the technical awareness needed to stay ahead of cybercrime.

• **Incident response program.** Perhaps the most famous example was the swift and transparent handling by Johnson & Johnson of the Tylenol deaths in 1982, which resulted in the development of tamper-resistant packaging. More recently, Home Depot's data breach response earned praise due to the fact that they notified their customers "even before they had fully confirmed the breach," according to an article on Tripwire by Ajmal Kohgadai.[10] (Like Target, Home Depot was hacked through malware installed by a third-party vendor.)

— **Broadcast awareness** is a process for quickly moving through triage on new incidents, measured by tests and incidents. The process should articulate what happens from the time an employee becomes suspicious to when the media is notified.

— **Forensic investigation.** When an incident is a result of a computer crime or has the potential of becoming part of a legal proceeding, evidence can be derived from computers and then used in court against the suspected individuals.

— **Notification process.** In the event a breach of security jeopardizes non-public financial or protected health information. This notification may affect individuals, the media, and law enforcement.

• **Third-party auditing** provides objective feedback on security procedures, guidance for improvement, and certification of federal compliance. But it's not a one-shot deal. Regular auditing and reporting ensures ongoing compliance in a perpetually shifting cyberworld.

• **Up-to-date cybersecurity insurance.** Despite all best intentions, data breaches can still occur, and yet are not covered by traditional liability insurance. It's imperative that vendors maintain up-to-date cybersecurity insurance that provides forensic investigation, media consultancy, and credit monitoring not only for your company, but for your customers as well.

10. Tripwire, "The Right Way to Respond to a Data Breach," https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-right-way-to-respond-to-a-data-breach. Accessed November 2017.

Reporting.

Complete automation is a myth. Humans will always be the ones at risk, they will always orchestrate the hacking, and they will always oversee and be accountable for the monitoring and reporting of information security. There are reporting tools, however, that can help bring some clarity to the process.

• **Service Organization Control (SOC)® reports** are designed to help organizations that operate information systems and provide information system services to other entities build trust and confidence in their service delivery processes and controls through a SOC report by an independent Certified Public Accountant.

Each type of SOC report[11] is designed to help service organizations meet specific user needs.

• **Statements on Standards for Attestation Engagements (SSAE).** SSAE 16 was drafted with the intention and purpose of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard (ISAE 3402). SSAE 16 also establishes a new Attestation Standard called AT 801 which contains guidance for performing the service auditor's examination.

• **Security Technical Implementation Guides (STIG).** Cybersecurity methodology implemented by the Defense Information Systems Agency (DISA) to enhance the security posture of the Department of Defense. Its goal is to standardize protocols throughout software, hardware, physical, and logical architectures and may cover router, firewall, and server configurations.

• **Compliance attestation report** represents a snapshot of the condition of an organization's information security posture, and regular audits performed by an objective third party are a critical component of long-term security. Bacompt has been found to be in compliance with HIPAA, GLBA, and FISMA.

Which SOC Report Is Right for You?[11]

Will report be used by your customers and their auditors to plan/perform an audit of their financial statements?	**Yes**	**SOC 1 Report**
Will report be used by customers/stakeholders to gain confidence and place trust in a service organization's system?	**Yes**	**SOC 2 or SOC 3 Report**
Do you need to make report generally available?	**Yes**	**SOC 3 Report**
Do your customers have the need for/ability to understand the details of processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	**Yes**	**SOC 2 Report**
	No	**SOC 3 Report**

11. American Institute of CPAs, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-reports-flyer-final.pdf. Accessed November 2017.

In conclusion.

Advancing technology gives businesses and consumers alike greater ease of use, vast amounts of information, increased efficiencies, and better overall service. But it has also opened up immense opportunities for cybercrime. While government and law enforcement are in a perpetual state of review-and-revise in an attempt to stay ahead of the electronic curve, criminals keep getting smarter.

That's why it's imperative that any third-party organizations with access to your data go through rigorous certification processes, provide proof of compliance, remain up to date on all mandates, and have more than adequate cybersecurity insurance.

Your company may have security protocols in place, but the essential question is how do your vendors (and their vendors) stack up?

About Bacompt

Data. Driven. Results.

Bacompt has been blazing the technology trail in high-security documents for over thirty years. As one of the first providers of high-volume digital printing, we've consistently pushed the boundaries of not only what we offer, but also what is possible.

High-security document processing.

- Healthcare, government, non-profit, collections, finance
- Statements, collection letters, tax documents, solicitations
- Online bill payment and presentment (OBPP)
- Data management, variable color printing, finishing
- List hygiene, presorting, inserting, mailing

Certified and compliant.

- FFIEC guidelines and HIPAA, GLBA, and FISMA compliant
- Third-party monitoring and annual DISA/STIG reviews
- Onsite USPS employee for daily mail validation and acceptance
- Rigorous data and physical security
- Strict background clearance for all employees
- DFAS (Defence Finance and Accounting Service) IT security clearance

BACOMPT

12742 Hamilton Crossing Blvd.
Carmel, IN 46032-5422
800-533-7109
www.bacompt.com