Information Security Law Update 2020

Dave Ries

dries@clarkhill.com
412.394.7787
D-Link Agrees to Make Security Enhancements to Settle FTC Litigation

Commission alleged the company failed to secure its routers and Internet-connected cameras

FOR RELEASE
July 2, 2019

TAGS: Technology | Bureau of Consumer Protection | Consumer Protection |
Privacy and Security | Consumer Privacy | Data Security | Tech

Smart home products manufacturer D-Link Systems, Inc., has agreed to implement a comprehensive software security program in order to settle Federal Trade Commission allegations over misrepresentations that the company took reasonable steps to secure its wireless routers and Internet-connected cameras.

The settlement ends FTC litigation against D-Link stemming from a 2017 complaint in which the agency alleged that, despite claims touting device security, vulnerabilities in the company’s routers and Internet-connected cameras left sensitive consumer information, including live video and audio feeds, exposed to third parties and vulnerable to hackers.
“As part of the proposed settlement, D-Link is required to implement a comprehensive software security program, including specific steps to ensure that its Internet-connected cameras and routers are secure. This includes implementing security planning, threat modeling, testing for vulnerabilities before releasing products, ongoing monitoring to address security flaws, and automatic firmware updates, as well as accepting vulnerability reports from security researchers. In addition, D-Link is required for 10 years to obtain biennial, independent, third-party assessments of its software security program.”
FOR IMMEDIATE RELEASE
November 27, 2019

OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information

In an agreement with the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), Sentara Hospitals (Sentara) have agreed to take corrective actions and pay $2.175 million to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification and Privacy Rules. Sentara is comprised of 12 acute care hospitals with more than 300 sites of care throughout Virginia and North Carolina.

In April of 2017, HHS received a complaint alleging that Sentara had sent a bill to an individual containing another patient’s protected health information (PHI). OCR’s investigation determined that Sentara mailed 577 patients’ PHI to wrong addresses that included patient names, account numbers, and dates of services. Sentara reported this incident as a breach affecting 8 individuals, because Sentara concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred. Sentara persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR. OCR also determined that Sentara failed to have a business associate agreement in place with Sentara Healthcare, an entity that performed business associate services for Sentara.
FOR IMMEDIATE RELEASE
October 23, 2019

OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System for HIPAA Violations

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services has imposed a civil money penalty of $2,154,000 against Jackson Health System (JHS) for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Breach Notification Rules between 2013 and 2016. JHS is a nonprofit academic medical system based in Miami, Florida, which operates six major hospitals, a network of urgent care centers, multiple primary care and specialty care centers, long-term care nursing facilities, and corrections health services clinics. JHS provides health services to approximately 650,000 patients annually, and employs about 12,000 individuals.

On August 22, 2013, JHS submitted a breach report to OCR stating that its Health Information Management Department had lost paper records containing the protected health information (PHI) of 756 patients in January 2013. JHS’s internal investigation determined that an additional three boxes of patient records were also lost in December 2012; however, JHS did not report the additional loss or the increased number of individuals affected to 1,436, until June 7, 2016.
Information Governance

Information Governance Reference Model (IGRM)
Linking duty + value to information asset = efficient, effective management

Duty: Legal obligation for specific information
Value: Utility or business purpose of specific information
Asset: Specific container of information
Minimize Data – Reduce Risk

- Inventory
- Classify
- Dispose/Delete
- Devalue
- Reduce Future Collection

From:
“Security Practices That Won’t Bust Your Budget”
Sherri Davidoff and Dave Ries, ABA TECHSHOW 2019
Security

Privacy
Defining Security Requirements

- Legal requirements
- Legal needs
- Business needs
Legal Requirements

Federal statutes and regulations
State statutes and regulations
Contracts
Common law – “reasonable security”
“Reasonable” “Appropriate”

1. Contracts
2. Legal / regulatory requirements
3. Standards / benchmarks / best practices
Standards and Frameworks

• NIST Framework
• NIST Special Publication 800-53, Rev 4 + numerous additional standards
• ISO 27000 series standards: Information Security Management Systems
NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Version 1.1 – April 2018
Standards and Frameworks

- U.S.-CERT: resources for SMBs
- **FTC: Small Business Resources**
Small Business

Announcing the Launch of the NIST Small Business Cybersecurity Corner Website

March 31, 2016
By: Kirsten Raymond

Existing NEWS from NIST: The Small Business Cybersecurity Corner Website is now live!

EMAIL ALERTS
sign up below to receive NIST blog updates.

STAY CONNECTED

CATEGORIES

After the signing of The NIST Small Business Cybersecurity Act in August of 2015, NIST got to work on the development of the Small Business Cybersecurity Corner to disseminate consistent, clear, concise, and actionable cybersecurity guidance to small businesses. NIST Director Dr.Fast Graph, just announced at RSA that our website has gone live.
The vast majority of small businesses rely on IT to run their businesses and to store, process, and...
“Top 20 Controls”

Center for Internet Security

*CIS Controls for Effective Cyber Defense Version 7.1*

= “specific and actionable ways to stop today’s most pervasive and dangerous cyber attacks.”

- “...updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources.”
**Recommendation 1:**
The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.
# Cybersecurity Framework

**April 16, 2018**

**Version 1.1**

## Table 2: Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IDENTIFY</strong> (ID)</td>
<td>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.</td>
<td>ID.AM-1: Physical devices and systems within the organization are inventoried</td>
<td>CIS CSC 1, CobiT 5 BA00.01, BA00.02, ISA 62443-2-1:2009 4.2.3.4, ISA 62443-3-2013 SR 7.8, ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, NIST SP 800-55 Rev. 4 CM-8, PM-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-2: Software platforms and applications within the organization are inventoried</td>
<td>CIS CSC 2, CobiT 5 BA09.01, BA09.02, BA09.05, ISA 62443-2-1:2009 4.2.3.4, ISA 62443-3-2013 SR 7.8, ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1, NIST SP 800-55 Rev. 4 CM-8, PM-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-3: Organizational communication and data flows are mapped</td>
<td>CIS CSC 12, CobiT 5 DSS05.02, ISA 62443-2-1:2009 4.2.3.4, ISO/IEC 27001:2013 A.13.2.1, A.13.2.2, NIST SP 800-55 Rev. 4 AC-4, CA-1, CA-9, PL-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-4: External information systems are catalogued</td>
<td>CIS CSC 12, CobiT 5 APO02.02, APO10.04, DSS01.02, ISO/IEC 27001:2013 A.11.2.6, NIST SP 800-55 Rev. 4 AC-20, SA-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value</td>
<td>CIS CSC 13, 14, CobiT 5 APO03.03, APO03.04, APO12.01, BA00.02, BA00.05, ISA 62443-2-1:2009 4.2.3.6, ISO/IEC 27001:2013 A.8.2.1, NIST SP 800-55 Rev. 4 CP-2, RA-2, SA-14, SC-6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and NIST Framework</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Informative References</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS CSC 1</td>
<td></td>
</tr>
<tr>
<td>CobiT 5 BA00.01, BA00.02</td>
<td></td>
</tr>
<tr>
<td>ISA 62443-2-1:2009 4.2.3.4</td>
<td></td>
</tr>
<tr>
<td>ISA 62443-3-2013 SR 7.8</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-55 Rev. 4 CM-8, PM-5</td>
<td></td>
</tr>
<tr>
<td>CIS CSC 2</td>
<td></td>
</tr>
<tr>
<td>CobiT 5 BA09.01, BA09.02, BA09.05</td>
<td></td>
</tr>
<tr>
<td>ISA 62443-2-1:2009 4.2.3.4</td>
<td></td>
</tr>
<tr>
<td>ISA 62443-3-2013 SR 7.8</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-55 Rev. 4 CM-8, PM-5</td>
<td></td>
</tr>
<tr>
<td>CIS CSC 12</td>
<td></td>
</tr>
<tr>
<td>CobiT 5 DSS05.02</td>
<td></td>
</tr>
<tr>
<td>ISA 62443-2-1:2009 4.2.3.4</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.13.2.1, A.13.2.2</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-55 Rev. 4 AC-4, CA-1, CA-9, PL-8</td>
<td></td>
</tr>
<tr>
<td>CIS CSC 12</td>
<td></td>
</tr>
<tr>
<td>CobiT 5 APO02.02, APO10.04, DSS01.02</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.11.2.6</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-55 Rev. 4 AC-20, SA-9</td>
<td></td>
</tr>
<tr>
<td>CIS CSC 13, 14</td>
<td></td>
</tr>
<tr>
<td>CobiT 5 APO03.03, APO03.04, APO12.01, BA00.02, BA00.05</td>
<td></td>
</tr>
<tr>
<td>ISA 62443-2-1:2009 4.2.3.6</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.8.2.1</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-55 Rev. 4 CP-2, RA-2, SA-14, SC-6</td>
<td></td>
</tr>
<tr>
<td>CIS CSC 17, 19</td>
<td></td>
</tr>
<tr>
<td>CobiT 5 APO01.02, APO07.06, APO13.01, DSS06.03</td>
<td></td>
</tr>
</tbody>
</table>
Security is a Team Effort!

Board
Executive Team
Managers
All employees
Customers
Service Providers & Contractors
Supply chain
Comprehensive Security Program

- Assignment of responsibility for security,
- An inventory of information assets and data,
- A risk assessment,
- Appropriate administrative, technical and physical safeguards to address identified risks,
- Manage new hires and current and departing personnel,
- Training,
- An incident response plan,
- A backup and disaster recovery program,
- Management of third-party security risks, and
- Periodic review and updating.
Addressing Risks

1. Apply security controls to **manage** the risk.
2. **Transfer** the risk (e.g., through an insurance policy or contract).
3. **Eliminate** the risk (by stopping the activity or doing it in a different way).
4. **Accept** the risk.
Cyberinsurance

• Relatively new area of coverage – starting in late 1990s
• Evolved during mid-2000s (as data breach notice laws took effect)
• 2016: 60+ carriers in U.S. – about $3.25 billion in premiums, expected to be $7.5 billion by 2020
• Specialty line of insurance – mostly nonstandard forms
• Variation in terms, coverage and exclusions
Protecting Privilege

Assessments and audits

Incident response
Laws Requiring Safeguards

Statutes

Regulations

Guidance

Federal + State
Laws Requiring Safeguards

Federal Information Security Management Act

Financial Industries Modernization Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

Children’s Online Privacy Protection Act
Laws Requiring Safeguards

Fair Credit Reporting Act (FACTA)
Sarbanes-Oxley Act
Family Educational Rights and Privacy Act
Federal Trade Commission Act
State Laws
SUPPLEMENTARY INFORMATION:

1. Introduction
   A. Cybersecurity

   Cybersecurity risks pose grave threats to investors, our capital markets, and our country.¹

¹ The U.S. Computer Emergency Readiness Team defines cybersecurity as "[t]he activity or process, ability or incapability, to secure information and communicational systems and the information contained therein are protected from and/or defended against damage, unauthorized use, or modification, or exploitation." U.S. Computer Emergency Readiness Team Website, available at https://www.us-cert.gov/glossary#id (Adapted from CNSI 0029, NIST SP 800-53 Rev.4, NSP, 2015 National Preparedness Goal, White House Cyberspace Policy, May 2015)
Federal Breach Notice

HIPAA
Gramm-Leach-Bliley Rules
Veterans’ Information

Proposed Laws
State Laws

Data Breach Notice    - 50
Credit Freeze         - 50
Reasonable Security   - 24
Encryption            -  2
Secure Disposal       - 35
SSN Protection        - 34
PCI Liability         -  3
State Breach Notice

Cal. Database Security Breach Notification Act

All 50 states

PA law 73 P.S. §2301-2329

List of laws:

“Doing Business”
State Breach Notice

- Information covered
- Entities covered
- Definition of “breach”
- Who must be notified
- Risk of harm
- Time of notice
- Form or method of notice
- Exceptions
  - Safe Harbor
  - Encryption
The New Year Brings New Data Breach Laws

Keisha M. McClellan, Melissa K. Ventronne | Data Privacy | Jan 10, 2020

Complying with changing state-level privacy laws will be a business priority in 2020. Because the United States does not have a uniform Federal privacy law, a patchwork of state rules based on where customers live poses new challenges to companies in the New Year. Here are seven (7) data breach updates in 2020 you should know:
IdentityTheft.gov can help you report and recover from identity theft.

**HERE’S HOW IT WORKS:**

1. **Tell us what happened.**
   We’ll ask some questions about your situation. Tell us as much as you can.

2. **Get a recovery plan.**
   We’ll use that info to create a personal recovery plan.

3. **Put your plan into action.**
   If you create an account, we’ll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

Get started now or you can browse a complete list of possible recovery steps.
Contracting for Security

“Reasonable security”
Detailed requirements
Incorporate standards

Third-parties / supply chain
Federal Enforcement

Federal Trade Commission
Dept. of Health and Human Services
Federal Communications Commission
Securities and Exchange Commission
Banking Agencies
Financial Industry Regulatory Authority
   (independent regulator)
Commodity Futures Trading Commission
Consumer Financial Protection Bureau
Encryption

Mass. Law - M.G.L. c. 93H

HIPAA

G-L-B

FTC
FTC Enforcement

Violation of laws & regulations

Misrepresentations or false promises
-“Deceptive trade practices”

“Unfair trade practices”
FTC Security Guides

PROTECTING PERSONAL INFORMATION

A Guide for Business

June 2015

October 2016
Dittman v. UPMC
Pa. Supreme Court
Nov. 21, 2018

JUSTICE BAER

DECIDED: NOVEMBER 21, 2018

We granted discretionary review in this matter to determine whether an employer has a legal duty to use reasonable care to safeguard its employees’ sensitive personal information that the employer stores on an internet-accessible computer system. We also examine the scope of Pennsylvania’s economic loss doctrine, specifically whether it permits recovery in negligence for purely pecuniary damages. For the reasons discussed below, we hold that an employer has a legal duty to exercise reasonable care to safeguard its employees’ sensitive personal information stored by the employer on an internet-
Additional Cases
Incident Response Plans

Preparing for **when** there will be a breach, not **if** there may be a breach

The new mantra in security:
Identify & Protect + **Detect, Respond & Recover**
Rapid Response
(Business E-mail Compromise)

1. Notify the bank – security group.
2. Notify the FBI or the Secret Service. (IRS)
3. Notify the FBI Internet Crime Complaint Center (IC3).
   General:  www.ic3.gov
   BEC/EAC:  https://bec.ic3.gov
5. Notify your insurer.
6. Determine point / method of compromise and secure.
7. Preserve evidence: e-mail headers, logs, etc.
Complaint Referral Form
Internet Crime Complaint Center

Please make every effort to complete the complaint form in its entirety as missing information could delay the freezing/recovery of funds and potential investigative efforts. The items in blue text and accompanied by a diamond (♦) are especially important in complaints where money was wired internationally and/or domestically. Providing financial information assists the FBI in locating funds for potential recovery and assists in preventing others from being further victimized.

Note: Fields marked with * are required.

Victim Information

* Name: 
Business Name: ♦
Age: Please select one... ▼
* Address: 
Address (continued):
Suite/Apt./Mail Stop:
* City: 
County:
* Country: Please Select One... ▼
State: [](State)
* Zip Code/Route: 
* Phone Number: numbers only (1112223333) ♦
* Email Address: jdoe@email.com ♦
Business IT POC, if applicable: Name, Email, Phone number, etc.
Other Business POC, if applicable: Name, Email, Phone number, etc.
Thank You!

David G. Ries
dries@clarkhill.com
412.394.7787

https://asset-360.com