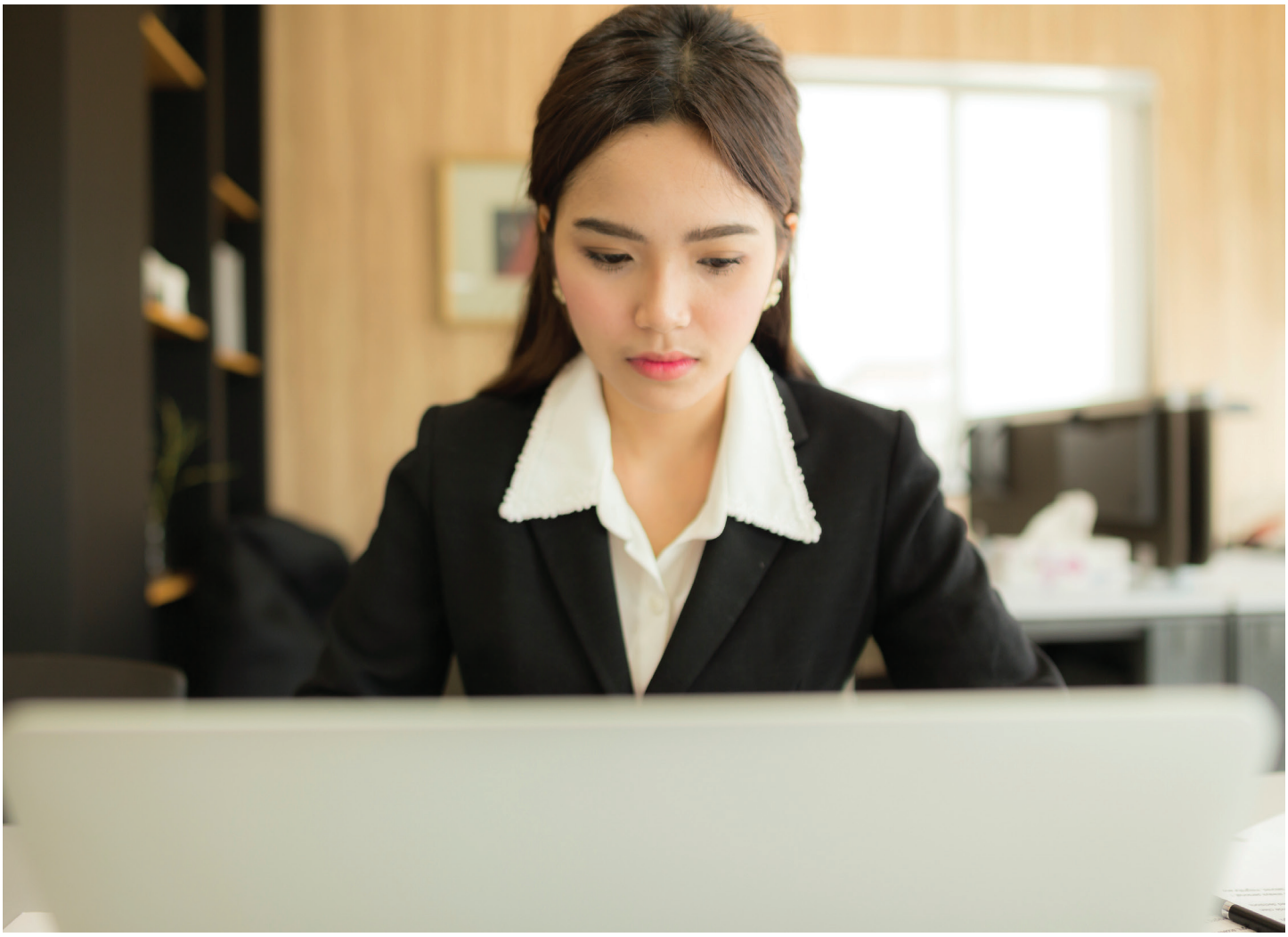
WELLS FARGO INSURANCE

White Paper: Technology, Privacy and Network Security

Employee-caused data breaches: Out of the office, but not off the grid

By Mario Paez and Kathleen Curley, Wells Fargo Insurance Professional Risk Practice

October 2015



Together we'll go far

Many companies agree that good employees are their most important asset. To be successful with employee retention, companies must remain aware of the top concerns of their workforce — which extend beyond competitive salaries and benefits.

For most employees, privacy is a paramount concern. The human resources department retains a wealth of personal and sensitive information about employees. Therefore, a data breach involving employee data can be the most damaging type of breach. To protect their networks and information, companies today are making extensive investments in information technology (IT). According to a Ponemon research report on 703 U.S. IT security practitioners involved in endpoint security, "Forty-five percent of respondents say their organization's IT security budget will significantly increase (12%) or increase (33%)."[1]

Employees are the #1 cause of security-related incidents

While breaches have many causes, employees themselves continue to be the #1 cause of security-related incidents. According to a 2015 Data Breach Industry Forecast by Experian, 59% of security incidents in the last year could be attributed to employees — human error and malicious insiders.[2] Malicious hacking remains the most expensive type, according to the 2015 Ponemon Cost of Data Breach Study.[3] In addition, another Ponemon study[4] found that:

- Nearly three-quarters (71%) of the employees surveyed said they had too much access to confidential company data.
- Fifty-four percent of the employees said their access to confidential data was frequent.
- Less than half (47%) of the employees said they believed their companies acted appropriately to protect the company data that employees access.

Due to advances in technology, we are more connected today than ever before. Today, employees are capable of accessing corporate networks and information from anywhere, anytime. They have the ability to connect through their personal or company devices via remote login (fobs and VPNs) over the internet, from anywhere in the world. As every aspect of the technology chain opens up the possibility of a breach, the exposure multiplies.

In this paper, we explore the recent trends in employee-related data breaches and measures to protect employee data, as well best practices and where insurance can assist.

Emerging trends for employees and data

Breaches have the potential to expose sensitive information, such as human resource, financial, and salary-related information, as well as medical history, personal emails, budgets, and trade secrets. The effects of such an event can lead to customer loss, reputational damage, and more.

Several emerging trends involving employees and data include:

- **Impostor fraud (also called fraudulent inducement or social engineering fraud).** Hackers use targeted email phishing and spear-phishing attacks to trick employees into clicking on malicious links (example: installing malware). Hackers gain access to computer systems, explore the data, and identify information that they want to steal, utilize, or potentially destroy.
    - Hackers send emails posing as certain individuals and request wire transfers.
    - According to the 2015 Verizon Data Breach Investigations Report (DBIR), "This year, 23% of recipients [are] now opening phishing messages and 11% [are] clicking on attachments."[5]
- **Human activity.** Employees act negligently or perform malicious acts.
- **Unauthorized access.** Employees access unauthorized parts of a company's network or facility.
    - According to the Verizon DBIR, 55% of insider incidents involved privilege abuse.
        - Employees often plan to sell stolen data or to directly compete with a former employer.
- **Remote access.** Bring Your Own Device (BYOD) environments, use of non-secure Wi-Fi connections, and employees sharing devices with others can all create exposures for possible breaches.

Recent breaches illustrate far-reaching impacts

The cases below, which made recent headlines, highlight the concerns and potential damages associated with a data breach.

U.S. Government's Office of Personnel Management (April and June 2015)[6]

The personal data, including information such as names, dates of birth, addresses, and Social Security numbers, of 4.2 million current and former federal government employees were stolen. Affected individuals were notified. While investigating the April incident, it was discovered that additional background investigation records (including Social Security numbers, usernames, and passwords) of 21.5 million current and former federal government employees were stolen, with cyber espionage being the suspected cause. Notifications for the second incident are expected.

Rady Children's Hospital, San Diego (June 2014)[7]

In two incidents over two years, an employee erroneously emailed the protected health information (names, dates of birth, medical diagnoses, medical record numbers, insurance carriers, and claims information) of more than 20,000 patients to job applicants. The employee, who had authorized access to the data, actually intended to send a training file to evaluate the applicants. Affected individuals were sent notification letters, and the hospital worked with an outside security forensics firm to ensure deletion of the data.

Best practices to help prevent a breach or mitigate its impact

To prevent a potential breach, or reduce the impact of a breach, best practices and preventive measures can go a long way. Some practical measures with respect to employees include:

- Perform background checks on employees, especially on individuals who handle sensitive information.
- Institute "clean desk" policies for employees, ensuring secure physical locations for devices both during and outside of standard work hours.
- Institute need-to-know policies, restricting access to sensitive information and databases solely to employees who need that information.
- Institute record retention policies, limiting the time during which employees have access to certain sensitive information.
- Evaluate your mobile device management, procedures, and requirements (BYOD considerations) and employ multi-level verification to ensure that only authorized people have access to data and systems.
- Employ interactive software that prevents or warns the sender when he or she is sending confidential information outside of the organization.

Additional best practices include:

- Encouraging the C-suite to treat network security and privacy as top priorities and make them part of the corporate culture.
- Providing thorough training to employees on their responsibilities with regard to information — a crucial step. The insurance marketplace has also become more proactive in offering loss-mitigation services, such as anti-phishing training for employees.
- Ensuring that employees understand the various sensitivity levels of information, and also how they should access information, in order to protect and use it in their daily tasks.
- Ensuring that employees are knowledgeable about the company's guidelines and have a general understanding about what to do and whom to contact internally in the event of a suspected data breach incident.

Risk transfer solutions can help protect your business

Comprehensive risk transfer programs typically include protection for:

- Network security and privacy liability
- Network extortion
- Electronic media liability
- First-party business income loss and electronic data restoration expenses
- Regulatory defense, fines, and penalties
- Payment card industry (PCI) penalties, fines, and assessments
- Consumer redress funds

How can we help?

As experienced brokers, Wells Fargo Insurance's Technology, Privacy and Network Security team can discuss your potential exposures and work with vendors to help you set up an incident response plan, provide a network assessment, and obtain the right insurance coverage.

For more information regarding this topic, please contact your Wells Fargo Insurance sales executive, or:

Mario Paez
952-242-3006 | mario.paez@wellsfargo.com

Kathleen Curley
917-368-6888 | kathleen.curley@wellsfargo.com

[1] 2015 State of the Endpoint Report: User-Centric Risk, January 2015.
http://www.ponemon.org/local/upload/file/2015%20State%20of%20Endpoint%20Risk%20FINAL.pdf

[2] 2015 Data Breach Industry Forecast, Experian, December 2014.
http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf

[3] 2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2015.
http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html

[4] "Corporate Data: A Protected Asset or a Ticking Time Bomb?" Sponsored by Varonis, independently conducted by Ponemon Institute LLC, December 2014.
http://info.varonis.com/hs-fs/hub/142972/file-2194864500-pdf/ponemon-data-breach-study.pdf?&__hssc=&__hstc&hsCtaTracking=c771f50d-6a90-42c2-97d0-868ac3bcfc5b%7C510f5a1e-60a8-4304-b497-8ec886f3ca3c

[5] 2015 Data Breach Investigations Report, Verizon, April 2015.
http://www.verizonenterprise.com/DBIR

[6] U.S. Office of Personnel Management.
https://www.opm.gov/cybersecurity

[7] "Employee gaffe causes 2 data breaches," *Healthcare IT News*, June 2014.
http://www.healthcareitnews.com/news/employee-gaffes-cause-two-HIPAA-data-breaches

This advisory is for informational purposes and is not intended to be exhaustive nor should any discussions or opinions be construed as legal advice. Readers should contact a broker for insurance advice or legal counsel for legal advice.

Products and services are offered through Wells Fargo Insurance Services USA, Inc., a non-bank insurance agency affiliate of Wells Fargo & Company, and are underwritten by unaffiliated insurance companies. Some services require additional fees and may be offered directly through third-party providers. Banking and insurance decisions are made independently and do not influence each other.

© 2015 Wells Fargo Insurance Services USA, Inc. All rights reserved. WCS-1353702