Security Essentials for Project Managers: Protecting Email and Mobile Devices[1]

Neil Farquharson, PMP

Abstract

Cyber-crime and espionage attacks your employers' or clients' reputation, profitability and future. Still somewhat quaintly referred to as "hacking," these threats are now foremost in corporate strategic thinking. With the security breaches at the U.S. Office of Personnel Management, Sony, Home Depot and many others, and the Edward Snowden revelations about message interception, senior executives are realizing that data security is no longer an issue to be decided solely by the IT department. It is a decision to be made and budgeted for in the boardroom. Project managers have unprecedented access to all levels of an organization including the C-Suite, and so not only have an influence over the design of business security processes, but also may be called upon at short notice to brief senior executives on data security issues, and even to make recommendations.

This paper seeks to identify vulnerabilities for corporate data loss and finds that data in transit across the public Internet and via mobile devices are the main mediums for data interceptions. It also highlights process weaknesses and human behaviors that expose these vulnerabilities.

Introduction

Executive boards across all industries continue to struggle to understand cybersecurity risks. According to a recent survey, just 11% of board members say they have a "high level" of knowledge about the topic.[1] While an earlier study by the National Association of Corporate Directors yielded the results graphed in Figure A. These were the ratings board level directors gave themselves around the time that the Anthem and other high profile data breaches were elevating concern about cybersecurity risks firmly into the boardroom.

[1] *Second Editions are previously published papers that have continued relevance in today's project management world, or which were originally published in conference proceedings or in a language other than English. Original publication acknowledged; authors retain copyright. This paper was originally presented at the 9th Annual University of Texas at Dallas Project Management Symposium in August 2015. It is republished here with the permission of the authors and conference organizers.*

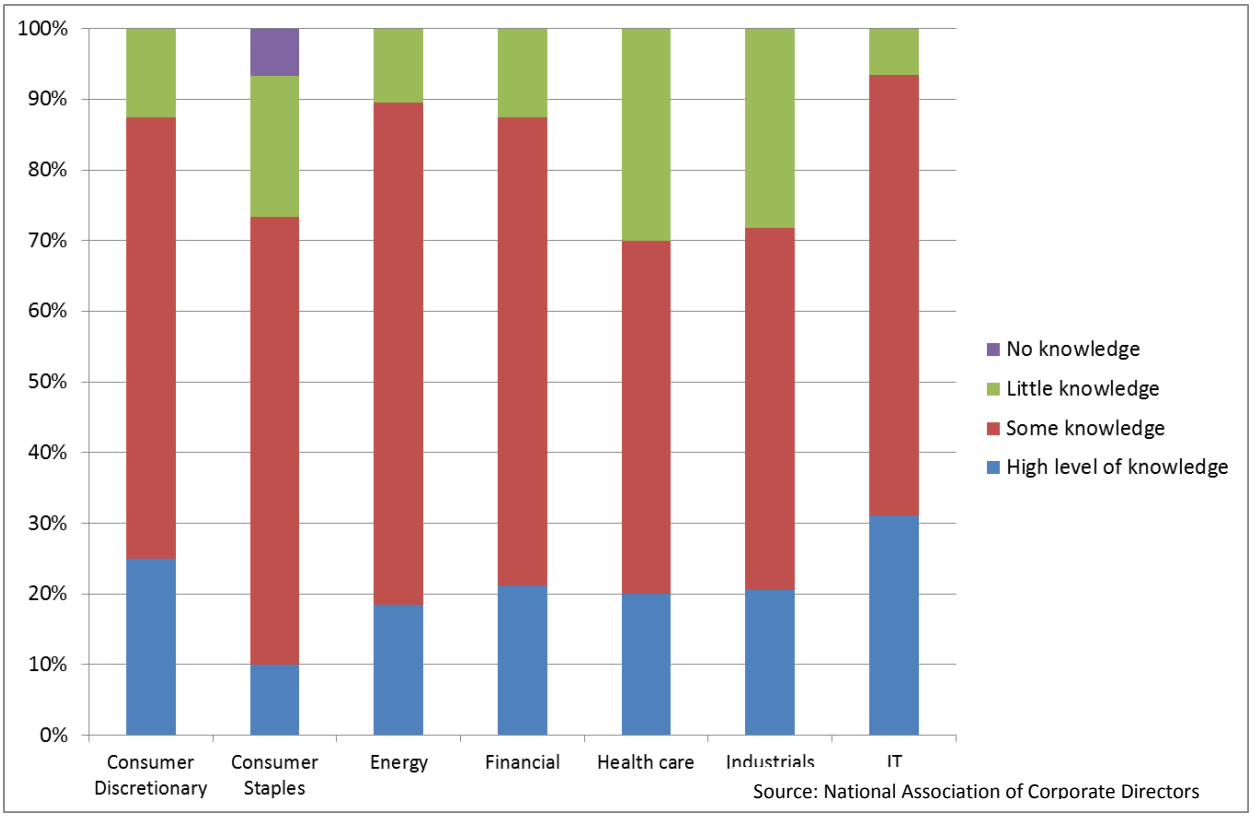

Figure A. How directors across sectors rated their own knowledge of cybersecurity risks

No More Complacency

Until recently, senior executives and boards of directors have often been complacent about the risks posed by data breaches and cyberattacks. However, there is an obvious growing concern about the potential damage to brand reputation, class-action lawsuits and costly downtime that is motivating executives to pay greater attention to the security practices of their organizations. No longer can the C-Suite leave security issues up to the IT department. They are hiring CISOs (Chief Information Security Officers) as fast as they can find qualified candidates; and paying increased salaries to attract them. Often they seek informed opinion from any third-party professional contact with knowledge of security issues, and project managers can find themselves being asked to offer such opinion. Although there is a multitude of cybersecurity risks, project managers should make themselves aware of the three major agents that cause breaches, and the vulnerabilities that can be exploited, or innocently compromised.

Three Typical Examples of Data Loss

1. On June 4th, 2015, the Office of Personnel Management (OPM), effectively the human resources department for the U.S. Government, confirmed that almost

four million current and past employees had been affected by a massive security breach.[2] That estimate would later rise to 21 million[3] and force the resignation of the Director.[4]

2. Then on June 23rd, the Securities and Exchange Commission (SEC) revealed that it is investigating a group of hackers who appear repeatedly to have broken into email systems at biotech and healthcare companies to gain financial advantages by trading in these companies' stocks.[5]

3. While in May, 2015, an employee at the Bank of England – the central bank of the United Kingdom – accidentally emailed highly sensitive government information to the wrong people.

These three examples are representative of threats to corporate, organizational and government sensitive data and intellectual property that can be perpetrated using our communications network. In the first example, suspicion has settled on the perpetrator being an agency working on behalf of a foreign government.[6] In the second example the perpetrator is believed to be well funded, well-educated organized crime, working out of North America or Western Europe, and motivated to make money – lots of money.[7] While in the third example, there was no crime committed per-se: The data loss came from the foreseeable human error of an employee, and due to a lack of management systems analysis. In other words, this is a human behavior that could have been anticipated based on the system in which the employee was working.

There are other groups that work to steal confidential information, an example being hacktivists, people who seek to advance an ideology or belief system for no personal gain. However most of these groups are a nuisance to businesses rather than executing the theft of sensitive information. DDoS attacks[8] are an example of such nuisance activities.

Where are the Risks?

In a 2015 survey of healthcare organizations,[9] respondents were asked the question: What do you perceive to be the single biggest emerging security threat your organization will face in 2015?

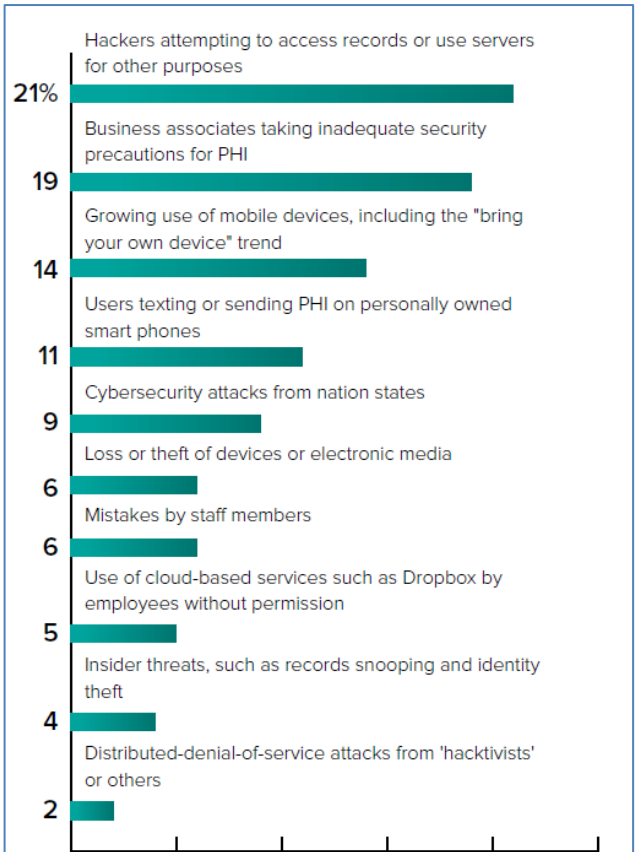

Figure B. The single biggest emerging security threat your organization will face in 2015.

While the top response was as expected, the second two top responses were: *business associates taking inadequate security precautions to secure protected health information (PHI)*; and the *growing use of mobile devices, including the bring your own device (BYOD) trend*.

The roles of business associates has come under scrutiny over the last few months[10] not least because of investigations into the massive ($191 million[11]) Target breach of 2013 where it is believed the breach began with the compromised emails of an HVAC firm based in Sharpsburg, Pensilvania.[12]

Business owners are often surprised that most breaches do not come from brute force attacks on firewalls but from combinations of social engineering and email interceptions. In his book, *Ghost in the Wires*,[13] Kevin Mitnick, formerly of the FBI's Most Wanted list, describes how easy it is for him to penetrate test the networks of modern day corporate clients. Very few of his techniques involve high technology, but usually involve circumventing security measures in deceptively simple ways. For example, he describes hiding out in a corporate client's car park with an ID badge that he has printed at home to look similar to the corporate badges worn by employees, but without the integral RFID[14] radio transponder of a real badge. When a group of smokers goes back in a side door, he follows them in in what is called "tailgating" and when the last employee looks at him, the employee sees the right kind of badge and gives Mr. Mitnick admittance. Once inside the building, Mitnick describes finding a target computer and, rather than defeating the security measures, he simply boots the computer from his own media – a CD ROM or USB drive – thus having access to the computer's operating system and root directories. Once he has remote control of the machine, he wipes records of his activities and leaves the computer as he found it: with one exception, the computer is now a remote slave to his own laptop back at base. He can now come and go inside the corporate firewall at will.

In a recorded interview from April 2015,[15] Mitnick demonstrates how easy it is to intercept emails as they pass between sender and recipient. It is called a man-in-the-

middle attack and there are many ways to achieve this: via copper wires in a traditional LAN; via insecure WiFi in hotels and cafés; and, as he demonstrates in the April video, by reading traffic on fiber-optic cables. What is particularly concerning about man-in-the-middle attacks is that under normal circumstances, these attacks are undetectable: The emails can be collected and scanned at-will for months or years without the victims ever becoming aware of the data leak. Only a few interceptions are ever detected, and these are only if the man-in-the-middle makes alterations to the text of an email before it is received by the recipient. For example, in 2014 an email between two financial professionals acting on behalf of the buyer and seller of a house exchanged wire transfer banking details in an unencrypted email. The email arrived 100% intact but with the receiving bank account number changed. Hence with just one email alteration $250,000 was stolen and never recovered.

The growing use of mobility devices, both corporate owned or personally owned (BYOD[16]) is causing concern to CISOs and the C-suite in most industries. The problem is that mobility devices, seven-inch and eleven-inch tablets and four to six-inch smartphones, are almost exclusively designed as consumer devices and not as corporate devices. These consumer devices are purposely designed to be *seamless*. For example, we can take a photograph and immediately upload it to Facebook or similar without going through any additional security checks; or we can open an emailed document and work on it in a word processing or spreadsheet application just as we would on a desktop computer. These functionalities offer great advantages to the corporation. It means that employees can work on almost any device, anywhere and at any time, including on a train or bus, or while waiting in an airport. This versatility has greatly increased the productivity of corporate employees, plus the employees themselves like the convenience of connecting to the office without being at the office and, in the case of BYOD, enjoy carrying one device only; the same device on which they can enjoy their favorite music, TV shows, audiobooks and social media, and carry their family photos. However this increased productivity and business versatility introduces a significant security flaw. The same seamlessness that makes the devices easy to use also allows criminals to leverage one application to compromise the whole device, or the corporate applications stored on that device.

The Double Edged Sword

corporate and BYOD solutions are managed by Mobile Device Management[17] or MDM. MDM comes under many names including EMM, MAM and *containerization*, however they all aim to achieve the same objectives: managing mobile devices to implement corporate data segregation, the securing of emails, securing corporate documents on the device and enforcing corporate policies. This means that a corporate application (app) to track customers can coexist with a personal social media app that maintains contact with friends and family; corporate documents can be edited in a corporate app but cannot be forwarded using a personal email app, and so on. Unfortunately for MDM, whole communities have grown up online around the concepts of *jailbreaking*[18] and

rooting[19] mobile devices. In improving jailbreaking and rooting programs, hobbyists, opportunist thieves and organized crime commingle together online and share methods for defeating the native security of mobility devices and bypassing the added security features of MDM. In doing so, they can gain access to any corporate data stored in the devices.

The traditional way that businesses respond to lost and stolen devices is the remote wipe:[20,21] An instruction is sent to the missing device that instructs it to delete all the corporate data or all data, both corporate and personal, that is stored on the device. This instruction is sent over the standard network and is therefore delivered either by cell technology or by WiFi, both of these being radio technologies. And therein lies the problem: a thief can isolate the device very quickly by simply switching it off, activating *Airplane Mode*, or by removing the battery. In a short video that can be viewed here[22], this author demonstrates how simple it is to isolate a mobility device so that no radio instructions can be received by the device.

A Faraday cage or Faraday bag is an enclosure made of conductive material that channels radio signals along and around the enclosure, without penetrating it. Faraday bags can be bought online[23] for $50 to $100, however wrapping the mobility device in aluminum kitchen foil achieves the same effect at a lower cost. Once a criminal isolates his stolen devices, he can take them back to his base and place them inside a larger Faraday case and connect them to his jailbreaking computer, hence the devices can be jailbroken or rooted without a remote wipe instruction ever being executed.

Human Behavior

Returning to Figure B, we see that the fourth concern of the surveyed healthcare organizations was that of employees sending sensitive information in the clear (not encrypted) using texting or similar messaging. As in the case of the Bank of England breach above, this is a human behavior predicated by the system in which employees are working. In the case of healthcare organizations, it is probable that the employees are not sharing sensitive information with the intention of exposing it to criminals, but because patients need assistance and available time is short. Often referred to as the *work-more economy,*[24] it is widely believed that since the recession began in 2007 employees in many organizations have been expected to do more work so that businesses can return to 2007 volumes without returning to 2007 staffing levels.[25] Thus given a situation where message encryption is not automated, staff have a choice

between keeping data secure, or fulfilling their work role, but not both. Therefore under such organizational systems it is a certainty that sensitive data will be exposed. In the Bank of England case, it is reported that staff now are obliged manually to type in all email addresses rather than using any automated functionality.[26] It is self-evident that this policy will severely slow down operations, however it still does not remove human error from the equation: A person can still type in a wrong email address to send sensitive information to.

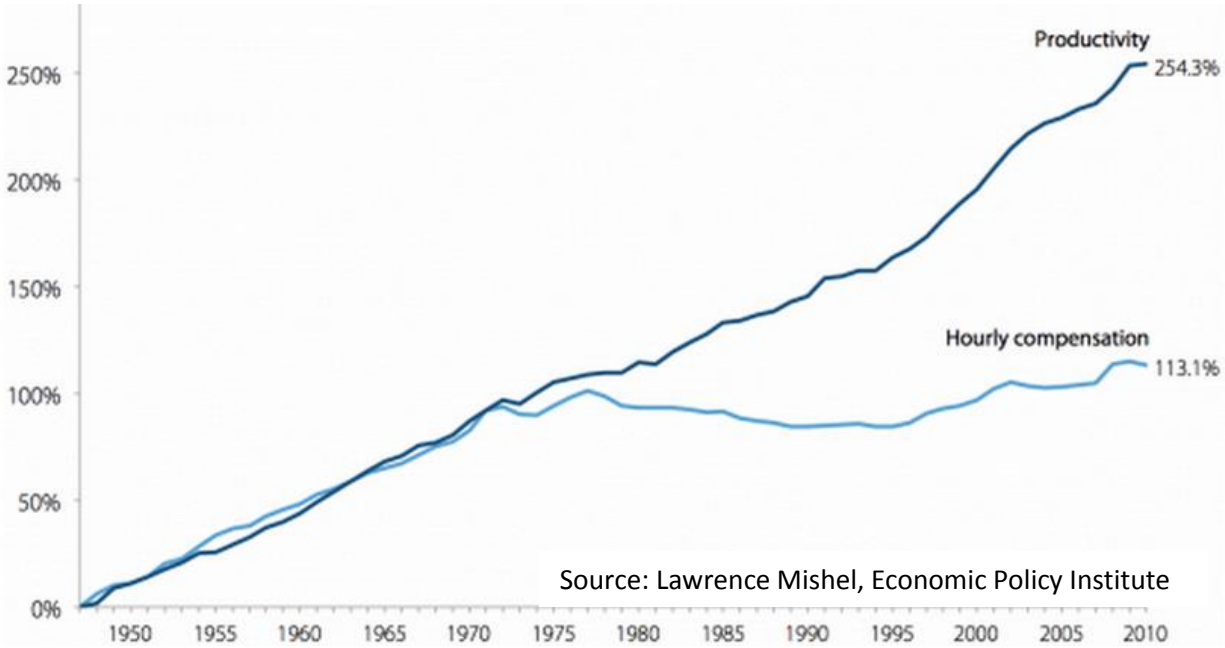

Figure C: Cumulative growth of hourly compensation and productivity, 1948 to 2011[27]

The Cost of Data Breaches

According to Larry Ponemon of the Ponemon Institute, the average cost of a data breach is now $154 per compromised record.[28] Here are some examples of costs:

- Anthem breach will probably cost the company in excess of $100 million[29]
- Target breach greater than $162 million[30]
- Sony breach is estimated at between $150 and $300 million[31]

Gartner estimates global losses from cybercrime total nearly $400 billion annually.[32] Cyber insurance may seem like the answer; however insurers will not write a blank check for organizations that do not have effective security in place. In 2013, California healthcare provider Cottage Health System inadvertently disabled security on one of its servers, exposing tens of thousands of patient files to the Internet. Cottage's insurer, Columbia Casualty, filed a suit against Cottage claiming it failed to follow "minimum required practices" and refused to pay.[33]

It is axiomatic that organizations must maintain an effective firewall around their servers and local area networks (sometimes referred to as a company Intranet). However the vast majority of breaches are accomplished by user credentials being harvested from unsecured emails as they transit the public Internet. Idan Tendler is a former agent of Israel's cyberwarfare specialist group. Speaking shortly after the U.S. Office of Personnel Management (OPM) breach, he stated:

"It's really no surprise that the OPM breach was traced back to a compromised credential as this is the case in nearly 80% of the breaches we have seen, including Target and Anthem. Compromised users continue to create great challenges for security teams. With legitimate access, it is difficult to detect whether an employee's actions are actually being perpetrated by that employee or by an outside source."[34]

according to the 2014 US State of Cybercrime Survey, “While organizations are more concerned about cyber threats, our research finds they have done very little to strategically invest in cybersecurity and ensure that it is aligned with the overall business strategy.”[35] Famously, it is alleged that in November 2005 Jason Spaltro, executive director of information security at Sony Pictures Entertainment, told a worried security auditor “I will not invest $10 million to avoid a possible $1 million loss.”[36] It also does not help that IT Security budgets are often lumped in with a company’s IT spend: If the CISO is subordinate to the CIO, it is quite likely that next year’s proposed IT projects will be compared to the proposed IT security projects and the latter projects will lose out

because it is easier to quantify the ROI for achieving business goals than it is to prevent a potential data breach.

However it should be noted that some senior executives have exhibited knee-jerk reactions[37] as they insist on extreme levels of protections that are usually cost prohibitive. One such example is to encrypt everything. Project managers who are asked about this should respond with three key pieces of information.

Firstly, encrypted information *at rest* (stored) is very costly and time consuming to archive and to search. Think also about eDiscovery[38] in the case of litigation – how does the system read millions of documents if every one of them must be decrypted before being scanned?

Secondly, if employees were forced to encrypt and decrypt every file, every communication, how long would it be before they would start to complain? And even if executives could overlook employee complaints, perhaps the wasted hours of productivity would jolt them back to reality.

Lastly, it is agreed by security experts that criminals' preferred modus operandi is to hijack existing privileged user accounts to gain access to the information they want. That is, the compromised privileged user accounts would give access to the encrypted data anyway, in which case encrypting data *at rest* would be no barrier to the criminals.

So just how do criminals get a hold of user credentials? There are some exotic James Bond style ways of obtaining credentials, and earlier in this paper mention was given to the real-life hacker and now corporate consultant Kevin Mitnick *tailgating* legitimate employees into their workplace. However these kinds of activities are not only expensive in time and effort, but also highly risky to the operative tasked with such activities. Instead criminals choose to work anonymously and safely in locations from which they can intercept confidential information as it transits the network. That is, as it travels over the public Internet; and unsecured email is their favorite first point of insertion. Of potential targets, Gartner states:

"[Organizations] that search for sensitive or private information in email often find it. However, exchanging this content with third parties is often a business imperative, and blocking it outright is rarely an option. Encryption becomes an enabling tool to send sensitive content safely and in compliance with regulations."[39]

Recommendations

1. Encrypt emails containing sensitive data as they transit the Internet.

2. Use an automated encryption system that detects the inclusion of sensitive data within an email. Do not rely on busy employees to make encrypt/don't encrypt decisions on a regular basis.

3. Systems should include state-of-the-art *lexicons*. That is, the system should search for text combinations that accurately discriminate between sensitive and non-sensitive information.

4. To prevent the accidental sending of sensitive information by employees, data loss prevention (DLP) measures should be implemented. Automated policy filters can determine whether the addressee is an authorized recipient for each type of information.

5. The use of BYOD devices that rely upon MDM solutions should be restricted only to staff with a clear requirement, such as outside sales staff and executive management.

6. Staff utilizing MDM should receive in-depth training in preventing loss or theft of their BYOD devices.

7. For the remainder of employees, a *secure viewer* BYOD solution will fulfil their needs. A secure viewer BYOD solution provides the required functionality without any corporate data residing on the BYOD devices.

Summary

There are three primary agents that have the potential to actively or misguidedly compromise organizations' information security: foreign agents working to steal intellectual property or corporate secrets; organized crime seeking to steal saleable information such as banking details, or client/employee personal information; and the organization's own employees. The primary first point of access is unsecured emails transiting the network. Under normal circumstances, emails are exposed once they leave the organization's local area network and begin to traverse the public Internet. Therefore while emails should not be encrypted while at rest, project managers should recommend that they be encrypted while in transit until they enter the local area network of the recipient.

A second exposure point exists where mobility devices are being used by employees to connect to their organization's mail server. MDM technology is a very versatile tool, but has an unresolved security issue. Hence project managers should recommend that only

sales and senior executives be authorized to use MDM, and that they be thoroughly trained in protecting their BYOD devices from loss or theft. All other employees should be compelled to use a secure viewer solution that does not allow storage of corporate sensitive information, or company emails on the device, thus protecting against loss of corporate data should these devices be lost or stolen.

References

1. "Boards Struggle With Cybersecurity, Especially in Health Care." The Wall Street Journal. Web. July 1, 2015
2. Sanger, David E. and Davis, Julie Hirschfeld. "Hacking Linked to China Exposes Millions of U.S. Workers." The New York Times, June 4, 2015. Print
3. "Information about OPM Cybersecurity Incidents." OPM.gov. Web. Recovered July 12, 2015
4. "Huge data breach prompts resignation of top US official." BBC News. Web. July 10, 2015
5. Moon, Mariella. "SEC investigates financial hackers attacking biotech firms." engadget.com. Web. June 24, 2015
6. Perez, Evan and LoBianco, Tom. "OPM inspector general questioned over hacking report." CNN. Web. June 17, 2015
7. "SEC Hunts Hackers Who Stole Corporate Emails to Trade Stocks." Reuters. Web. June 23, 2015
8. "Denial-of-service attack." Wikipedia. Web. Recovered July 12, 2015
9. "Healthcare Information Security Today." Information Security Media Group. June 2015. Print
10. Ibid
11. Robinson, Teri. "Target breach costs company $191M, financials show." SC Magazine. Web. February 25, 2015
12. Picchi, Aimee. "Target breach may have started with email phishing." CBSNews.com. Web. February 13, 2015
13. Mitnick, Kevin David. Ghost in the Wires. Little, Brown and Company, 2011. Print
14. "Radio-frequency identification." Wikipedia. Web. Recovered July 12, 2015
15. "The World's Most Famous Hacker Tells All: Email Hacks And Data Security." Video. Web. Recovered July 12, 2015
16. "Bring your own device." Wikipedia. Web. Recovered July 12, 2015
17. "Mobile device management." Wikipedia. Web. Recovered July 12, 2015
18. "iOS jailbreaking." Wikipedia. Web. Recovered July 12, 2015
19. "Rooting (Android OS)." Wikipedia. Web. Recovered July 12, 2015
20. "How to use Outlook Web App to remotely wipe an ActiveSync device in Office 365." support.microsoft.com. Web. Recovered July 12, 2015
21. "iCloud: Erase your device." Support.apple.com. Web. Recovered July 12, 2015
22. "Remote Wipe Instruction Demo." youtube.com. Recovered July 12, 2015
23. "Black Hole Faraday Bag" for sale on Amazon.com. Recovered July 12, 2015
24. Frauenheim, Ed. "Today's Workforce—Pressed and Stressed." Workforce. Web. December 16, 2011
25. Frauenheim, Ed. "A Bad Place to Be: In Denial About What Workers Want." Workforce. Web. October 27, 2011

26. Heritage, Stuart. “Undo... undo! The Bank of England is right to ban autocomplete emails.” The Guardian. Web, June 15, 2015
27. Mishel, Lawrence. “The Wedges Between Productivity and Median Compensation Growth.” Economic Policy Institute Issue Brief, April 26, 2012. Web. Recovered July 12, 2015
28. Ponemon, Larry. “2015 Cost of Data Breach Study: Global Analysis.” May 27, 2015. Web. Recovered July 12, 2015
29. Orborne, Charlie. “Anthem data breach cost likely to smash $100 million barrier.” ZDnet.com. Web. February 12, 2015
30. Prince, Brian. “Target Data Breach Tally Hits $162 Million in Net Costs.” Security Week. Web. February 26, 2015
31. Lowrey, Annie. “Sony’s Very, Very Expensive Hack.” New York Magazine. Web. December 16, 2014
32. Wheatley, Mike. “Hidden costs of Sony’s data breach will add up for years, experts say.” Silicon Angle. Web. February 20, 2015
33. Vaas, Lisa. “We don't cover stupid, says cyber insurer that's fighting a payout.” Naked Security, sophos.com. Web. May 28, 2015
34. Heller, Michael. “Stolen passwords to blame for OPM breach; director may take the fall.” TechTarget.com. Web. June 25, 2015
35. “2014 US State of Cybercrime Survey.” PricewaterhouseCoopers. Web. May, 2014
36. Santus, Rick. “Sony Pictures' security chief once thought data breaches weren't a big deal.” Mashable.com. Web. December 5, 2015
37. Litan, Avivah. “What Healthcare needs to learn from Retail after the Anthem Breach.” Gartner Blog Network. Web, February 7, 2015
38. “Electronic discovery.” Wikipedia. Web. Recovered July 12, 2015
39. Firstbrook, Peter and Ouellet, Eric. “Magic Quadrant for Secure Email Gateways.” Gartner, August 10, 2011. Print

About the Author

Neil Farquharson, PMP

Technology Evangelist
Texas, USA

As Technology Evangelist for Zix, Neil Farquharson takes technical subjects and distills them down into easily understandable summarized forms. A former soldier, engineer and operations manager, he relocated from the U.K. to the U.S. in 2003. Since then, he has been a regular speaker at IT security and telecoms events.

Mr. Farquharson holds degrees from the University of Glasgow and the University of Texas at Dallas. He lives in Dallas with his wife and children.

Neil can be contacted at Neil.Farquharson@verizon.net