INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Protection of Data and Prevention: Advice for Chief Executive Officers, Managers, and Information Technology Staff

C. Matthew Curtin, CISSP

Date: 2017/11/17 22:00:53

Abstract

Call it cybersecurity, information security, data security, or information assurance; the world has a problem with it. Whatever your rôle in an organization, you are not only a part of the problem: you are a critical part of the solution.

First, we consider what is actually happening "out there," and how to define the problem. To a large degree what we see is a matter of mechanism being put to surprising uses. This is the essence of a *hack*, and not necessarily malicious.

Quickly turning our attention to malicious and unauthorized activity, we look at what organizations need to do to protect themselves. Critical elements include education, engagement, and management. Effective security strategies we present include running a program in-house and subscribing to a third-party program. Tactics that we discuss include various types of security assessment and technology evaluations.

Whatever the mix of strategy and tactics you use for your organization, remember that everything you do has an inherent element of risk. Your goal is not to make risk zero, but to make risk acceptable, given the return that you expect. Even when security failures occur, they can be managed, and need not be catastrophes—as long as you've properly managed risk along the way.

What Is Security?

Asking ten people what *security* means is a good way to get ten different and even incompatible answers. Informal surveys I have conducted as part of presentations have resulted in definitions that often refer to a lack of compromise, or even the absence of a threat.

I like the Russian word for security—*bezopasnost'*—because it means literally "without danger." The concept does not mean that there is no threat, or even that there is no failure. It means that the event does not present *danger*.

Even when it comes to computing this is by no means a new concept. The earliest computer systems were focused on utility for those who had physical access but it was not long before generalization of the electric computing machine function led to the development of operating systems and controls meant to protect privacy and security.[1] Recognizing the need for security and privacy was not enough: it became a whole area of research that led to the development and publication of principles that still apply even today.[2]

Despite the fact that we've got computer science literature on security and privacy going back fifty years and the billions spent on security products and services today, we find ever-growing accounts of data breach reports. Equifax in September 2017 announced a breach that could impact 143 million Americans.[3] That number represents almost ninety percent of the American workforce.[4]

While a good deal of attention is often given to technology in these breach scenarios, widely-accepted wisdom is that the biggest threat to an organization is its people. Commonly we hear that the biggest source of threat is the insider.[5] In truth when we consider the actions or inactions of people, the rôle of humans in data breaches becomes much more pronounced[6]—and that's not as a result of including the attackers.

Returning to the Equifax example, media outlets reported that an easily-guessed pair of credentials and an two-months-old unpatched vulnerability in the system left the system vulnerable to attackers.[7] I have seen no real discussion of the design of the system, such that a single flaw would allow for extraction of such a massive amount of data.

Both actions—including establishing credentials and the design and implementation of the system—and inactions—failure to change credentials and to patch known vulnerabilities—created the condition that made it possible for still other people—attackers—to make the system do things that its operators did not intend.

The result is a massive breach affecting 143 million Americans, tremendous liability for the company, and massive expense in an attempt to recover from the problem.[8]

Important questions remain. How much did Equifax spend to design, build, and operate its system? How much of that spend included security? Did technology staff fail to use what security dollars they had effectively? Did operations fail to see the utility

[1] James P. Titus. Security and privacy. *Communications of the ACM*, 10(6):379–381, June 1967. ISSN 0001-0782

[2] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, volume 63, pages 1278–1308, September 1975; and Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001

[3] Brian Krebs. Breach at equifax may impact 143m americans. Krebs on Security, September 2017. URL https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/

[4] Bureau of Labor Statistics. Labor force statistics from the current population survey. Web Site. URL https://data.bls.gov/pdq/SurveyOutputServlet?graph_name=LN_cpsbref1&request_action=wh. Accessed 16 Nov 2017

[5] IBM. 2016 cyber security intelligence index. IBM X-Force Research, April 2016. URL http://ibm.biz/2016CyberIndex

[6] Marc van Zadelhoff. The biggest cybersecurity threats are inside your company. *Harvard Business Review*, September 2016. URL https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

[7] Lily Hay Newman. Equifax officially has no excuse. WIRED, September 2017. URL https://www.wired.com/story/equifax-breach-no-excuse/

[8] Stacy Cowley. Equifax faces mounting costs and investigations from breach. New York Times, November 2017. URL https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html

in security? Did leadership fail to provide incentives to keep the system secure in the first place?

Answers to important questions might well lead to important lessons.

The Art of the Hack

When hearing the term *hack*, listeners might conjure an image of a dark figure hiding behind a computer, using it for ill. That is neither the original meaning, nor is it the most useful. In fact, 'hackers' as they are known today in computing came from a group of the Tech Model Railroad Club (TMRC) at MIT in the 1950s.[9] Hackers *create* use ingenuity to create clever solutions to hard problems—quick and effective solutions.[10] Playfulness is part of the hacker culture, which has led to hacks that are sometimes for no other purpose than to entertain, such as the 1982 MIT-Harvard football game in which a weather balloon suddenly began to inflate on the sideline of the field.[11]

An essential element of the hack is to use something in a surprising (and sometimes entertaining) way. In the context of cybersecurity, the media has unfortunately hijacked the term hacker and its rich history and applied it to one case: making a computer system do something its operators did not intend—and for malicious or unauthorized purposes.

Malicious and Unauthorized Activity

The issue that we're facing in the design, implementation, and operation of systems is not what they are supposed to do, but what they are capable of doing. Attacks often come from introducing data in a way that causes the computer, or a person who uses the computer, to do something unexpected and unauthorized.

Many studies are available on data breach and other unauthorized activity.[12] Data studied, methodologies, and conclusions differ, but in any case provide effective means to gain an understanding of what is actually happening out there.

While the balance of effective controls can vary depending on the types of security incidents suffered within an organization specifically or an industry more broadly, controls often fall into broad categories that are often grouped as *administrative*, *physical*, and *technical*.

Examples of administrative controls include policies that define what is to be protected and the standards that establish how critical information will be managed. Physical controls include things

[9] Tech Model Railroad Club. Hackers. URL http://tmrc.mit.edu/hackers-ref.html. Accessed 17 Nov 2017

[10] hacker. The New Hacker's Dictionary. URL http://catb.org/~esr/jargon/html/H/hacker.html. Accessed 17 Nov 2017

[11] Amar Toor. Watch this: Mit's adorably nerdy hack during 1982 harvard-yale game. The Verge, November 2012. URL https://www.theverge.com/2012/11/19/3665306/mit-harvard-yale-1982-weather-balloon-prank

[12] Chris Novak, Jeremy Bohrer, John Loveland, and John Grim. Verizon 2017 data breach digest: Perspectives on "the human element". In *RSA Conference 2017 Learning Labs*, 2017. URL https://www.rsaconference.com/writable/presentations/file_upload/lab4-r12_data-breach-digest-perspectives-on-the-human-element_copy1.pdf; C. Matthew Curtin and Lee T. Ayres. Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), Winter 2008-09. URL http://web.interhack.com/publications/breach-taxonomy/; and Lee T. Ayres, C. Matthew Curtin, and Thomas A. Ng. Standardizing breach incident reporting: Introduction of a key for hierarchical classification. *Systematic Approaches to Digital Forensic Engineering, International Workshop on*, 0:79–83, 2010. URL http://doi.ieeecomputersociety.org/10.1109/SADFE.2010.19

like management of space, physical locks, and how physical assets are managed. Technical controls include the things that we often think of when talking about cybersecurity: firewalls, cryptography, and all of those things in the computer.

Having such controls defined, however, is not enough. I offer three elements that must be present in any organization with a good security posture: education, engagement, and management.

Education is more than simple training for people to regurgitate critical details. Education is making sure that people understand the essential elements of the risk[13] that the organization faces, the rôle that they play in identifying and managing it, and practical guidelines that they can follow that will protect themselves and the organization.[14]

Engagement means treating security as an important element of how people go about their work. People do not engage with security when they don't understand it, when it gets in their way of doing legitimate activity, or when they perceive that the organization's leadership does not really care about security.

Management is about the activities that need to take place for security to work: Regular training for staff, regular patch application,[15] regular review of security during design and implementation phases of systems, and so on.

Whether these activities are run entirely internally, or with the help of partners who specialize in security is less important than ensuring that the organization has access to and makes use of such resources. Many types of security services are available, and which to choose is often a matter of understanding what you want to do with the results. Here are a few for consideration.

Penetration testing. This is an effective method for seeing how an organization detects and responds to security incidents. This is not the most effective method for finding weaknesses that should be addressed.

Vulnerability assessment. Largely-automated scanning activity can go a long way toward identifying where there are weaknesses in systems in operation. Missed patches, configuration errors, and other weaknesses can be found and typically addressed in a straightforward manner.

Security program assessment. This type of activity may also present as audit or preäudit work. Essentially this is about looking at a security standard and seeing what controls exist or are planned by comparison to a standard framework for security controls.[16]

[13] Joint Task Force Transformation Initiative. Guide for conducting risk assessments. NIST SP 800-30 Revision 1, September 2012. URL `http://dx.doi.org/10.6028/NIST.SP.800-30r1`

[14] Mark Wilson and Joan Hash. Building an information technology security awareness and training program. NIST SP 800-50, October 2003. [online] `http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf`

[15] Peter Mell, Tiffany Bergeron, and David Henning. Creating a patch and vulnerability management program. NIST SP 800-40 Version 2, November 2005. [online] `http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf`

[16] Joint Task Force Transformation Initiative. Security and privacy controls for federal information systems and organizations. NIST SP 800-53 Rev.4, April 2013. [online] `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf`; and ISO. Information technology—security techniques—code of practice for information security management. International Standard ISO/IEC 27002, 2005

Avoiding Catastrophe, Not 'Problems'

We often think of avoiding security failures. With systems as complex as they are, it's far better to think not in terms of avoidance of problems, but the identification and management of problems that ultimately lead to the avoidance of a catastrophe. Twenty years ago, research began in this area, looking at *survivable* systems.[17]

The question becomes what you can do personally to operate more securely, and to support the security of your organization.

Executives need to make important decisions including how much risk the organization is willing to bear. As is true of any investment, the greater the return expected on investment in information technology, the greater the risk that will be borne. In the end, how much will the organization spend to protect $1? Knowing this is critical to success, as is knowing which assets are to be protected, and how risk is to be managed. Where risk is identified, it can be accepted, mitigated through controls, or transferred to another party, such as contracting with an insurance carrier or perhaps a service provider.

Managers will need to take the high-level directives made by executives and turn them into actionable programs to manage activities that implement leadership's intentions. Published security frameworks, standards, and research can go a long way toward making investments well. Programs that manage activities in support of security will need to include metrics that show what the organization is doing, data that can be compiled and reported back to leadership on a regular basis.

Staff on the front lines will need to ensure that activities outlined by management are undertaken with due care. Where resource contention takes place—and it most certainly will—staff need to advise management of the contention, preferably while it has yet to arrive. Cybersecurity is itself a large discipline, and not everyone on staff will become a security expert. Staff will, however, need to ensure that resources for training are put to good use, that the intention of leadership is understood, that management's tools to implement leadership's intentions are used, and that their own work is organized in a way consistent with the organization's intent.

Everyone has a part to play in the protection of the organization. Knowing your part, playing it well, and allowing others to play their parts will go a long way to operating securely.

[17] Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, and Nancy R. Mead. Survivable network systems: An emerging discipline, November 1997. [online] http://www.cert.org/research/97tr013.pdf

Bibliography

hacker. The New Hacker's Dictionary. URL http://catb.org/~esr/jargon/html/H/hacker.html. Accessed 17 Nov 2017.

Lee T. Ayres, C. Matthew Curtin, and Thomas A. Ng. Standardizing breach incident reporting: Introduction of a key for hierarchical classification. *Systematic Approaches to Digital Forensic Engineering, International Workshop on*, 0:79–83, 2010. URL http://doi.ieeecomputersociety.org/10.1109/SADFE.2010.19.

Bureau of Labor Statistics. Labor force statistics from the current population survey. Web Site. URL https://data.bls.gov/pdq/SurveyOutputServlet?graph_name=LN_cpsbref1&request_action=wh. Accessed 16 Nov 2017.

Tech Model Railroad Club. Hackers. URL http://tmrc.mit.edu/hackers-ref.html. Accessed 17 Nov 2017.

Stacy Cowley. Equifax faces mounting costs and investigations from breach. New York Times, November 2017. URL https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html.

C. Matthew Curtin and Lee T. Ayres. Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), Winter 2008-09. URL http://web.interhack.com/publications/breach-taxonomy/.

Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001.

Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, and Nancy R. Mead. Survivable network systems: An emerging discipline, November 1997. [online] http://www.cert.org/research/97tr013.pdf.

IBM. 2016 cyber security intelligence index. IBM X-Force Research, April 2016. URL http://ibm.biz/2016CyberIndex.

Joint Task Force Transformation Initiative. Security and privacy controls for federal information systems and organizations. NIST SP 800-53 Rev.4, April 2013. [online] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

ISO. Information technology—security techniques—code of practice for information security management. International Standard ISO/IEC 27002, 2005.

Joint Task Force Transformation Initiative. Guide for conducting risk assessments. NIST SP 800-30 Revision 1, September 2012. URL http://dx.doi.org/10.6028/NIST.SP.800-30r1.

Brian Krebs. Breach at equifax may impact 143m americans. Krebs on Security, September 2017. URL https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/.

Peter Mell, Tiffany Bergeron, and David Henning. Creating a patch and vulnerability management program. NIST SP 800-40 Version 2, November 2005. [online] http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

Lily Hay Newman. Equifax officially has no excuse. WIRED, September 2017. URL https://www.wired.com/story/equifax-breach-no-excuse/.

Chris Novak, Jeremy Bohrer, John Loveland, and John Grim. Verizon 2017 data breach digest: Perspectives on "the human element". In *RSA Conference 2017 Learning Labs*, 2017. URL https://www.rsaconference.com/writable/presentations/file_upload/lab4-r12_data-breach-digest-perspectives-on-the-human-element_copy1.pdf.

Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, volume 63, pages 1278–1308, September 1975.

James P. Titus. Security and privacy. *Communications of the ACM*, 10(6):379–381, June 1967. ISSN 0001-0782.

Amar Toor. Watch this: Mit's adorably nerdy hack during 1982 harvard-yale game. The Verge, November 2012. URL https://www.theverge.com/2012/11/19/3665306/mit-harvard-yale-1982-weather-balloon-prank.

Marc van Zadelhoff. The biggest cybersecurity threats are inside your company. *Harvard Business Review*, September 2016. URL https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

Mark Wilson and Joan Hash. Building an information technology security awareness and training program. NIST SP 800-50, October 2003. [online] http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.