Staying Safe: Cyber Security for People and Organizations

Kenning Arlitsch, and Adam Edelman

Kenning Arlitsch & Adam Edelman (2014) Staying Safe: Cyber Security for People and Organizations, Journal of Library Administration, 54:1, 46-56 http://dx.doi.org/10.1080/01930826.2014.893116

Column Title: posIT

Column Editor: Kenning Arlitsch, Dean of the Library, Montana State University, Bozeman, MT
kenning.arlitsch@montana.edu

This JLA column posits that academic libraries and their services are dominated by information technologies, and that the success of librarians and professional staff is contingent on their ability to thrive in this technology-rich environment. The column will appear in odd-numbered issues of the journal, and will delve into all aspects of library-related information technologies and knowledge management used to connect users to information resources, including data preparation, discovery, delivery and preservation. Prospective authors are invited to submit articles for this column to the editor at kenning.arlitsch@montana.edu

Staying Safe: Cyber Security for People and Organizations

By Kenning Arlitsch and Adam Edelman

Introduction

Cyber security has been in the news again. Target and Neiman Marcus department stores both acknowledged in December 2013 that hackers had stolen millions of their customers' credit card data during the height of the holiday shopping season. A few months earlier Adobe suffered a security breach that also compromised the records of millions of its customers. These three crimes may have garnered the most press because of the sheer number of people whose personal information were put at risk, but many more data thefts occurred in 2013 and the losses are mounting.

Our increasingly interconnected world creates threats of cybercrime that pervade our work and private lives. Some experts warn that fraud is inevitable, with "90 percent of businesses falling victim to at least one security breach [in the single year that was reviewed]…making the threat from cyber attacks a near certainty" (Summers, 2011). Identity theft is only one possible fallout of data theft, but it is a nuisance at the very least and potentially much more serious than that. At the least victims are forced to change passwords and get new credit cards. At worst, when an identity is truly stolen it can be difficult to prove identity, and it can take months or years to rebuild documentation and credit scores. For organizations, the direct cost associated with notifications, providing credit monitoring, and lost revenue due to reputational damage can be counted in millions of dollars. Target's revenue and reputation suffered noticeable losses in the weeks following their hacking revelation (Cheng, 2013). These are costly concerns by any measure.

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

Some data theft is simply malicious or mischievous, but most of it occurs because it's lucrative. Personal information is valuable precisely because it doesn't change. Names, birthdates, mothers' maiden names and Social Security Numbers are intended as permanently assigned markers for the vast majority of us, and health, financial, academic and other records of our lives are keyed to those markers, giving them bedrock status. But identification goes even deeper. Fingerprints, retinal characteristics, blood type and DNA are truly permanent markers that can be used to uniquely identify us even if we've lost all our other assigned markers. Scarcity increases value, and there is nothing more scarce than the single occurrence of a type that identifies us as individuals. As more medical data is stored electronically it too becomes a target.

Identity theft is an acute personal result of data loss, but damage to the enterprise is also severe when computer systems are attacked or data are stolen. Cyber attacks can take core systems offline, causing losses to productivity. Software code can be copied to pirate a company's products. Key documents revealing business plans and intellectual property can be sold to competitors. As the "Internet of Things" expands, critical infrastructure such as the electrical grid, petroleum distribution, and the financial markets are all interconnected and potentially vulnerable to malicious acts. The gap between the virtual world and the physical world has been bridged – it's not just information that is at risk anymore. Cyber security is a serious issue, in both personal and work environments.

A Rash of Theft

2013 was notorious for data breaches in all sectors as "more than 740 million records were exposed in 2013… in 1,400 incidents," making it the worst year for the loss of data since tracking began in 2005 (Online Trust Alliance, 2014). President Obama called cyberthreats "one of the most serious economic and national security challenges we face as a nation" (Brynko, 2013) and a report by McAfee highlights the costliness of cyber security incidents and the fact that attacks are increasing (Baker & Waterman, 2010). Perhaps the biggest media stories of commercial data theft came at the end of the year when 70-110 million customers (the exact number is unknown) of Target were affected by the theft of credit card numbers, PINs, email and mailing addresses in a little more than two weeks following the Thanksgiving holiday. In January Neiman Marcus revealed that 40 million of its customers were affected in a similar cyber attack (Velasco, 2014). Three months earlier Adobe Systems said 3 million of its customers' personal data had been stolen in a hack of its internal database. But later it raised that number to 38 million (Perlroth, 2013) and some sources hint that as many as 150 million may have been affected (Levin, 2013). In addition to losing the personal information of its customers Adobe also admitted the hackers had stolen the source code to some of its major software products, which could lead to malicious attacks on those products and their users, as well as to software pirating that threatens Adobe's profits.

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

The commercial sector isn't the only target of malicious attacks; although the headlines tend to be less splashy the problem is clearly severe in education domains. The *Privacy Rights Clearinghouse* reported 45 data breach incidents in K-12 and higher education in 2013 and 717 incidents since 2005. These are only the incidents that were reported, and we in higher education may not fully appreciate the gravity of the situation; the *2014 Horizon Report* that discusses emerging technologies and their challenges makes no mention of cyber security (Johnson, Becker, Estrada, & Freeman, 2014). According to the *New York Times* higher education institutions have seen a significant increase in the number of attacks on their systems. Bill Mellon, the associate dean for research policy at the University of Wisconsin was quoted as saying that "90,000 to 100,000 attempts [to penetrate UW's systems] per day, from China alone," were being recorded. The article goes on to state that some universities are no longer allowing professors to take laptops to certain countries because of fears that they will be infected with malware that copies all data on the computer or that infects other local systems once the computer is brought back to the home institution (Perez-Pena, 2013). The large number of devices and significant bandwidth typically found on university campuses coupled with a reputation for openness (i.e. lax security practices) make higher education a prime target for malicious actors. University networks are used as both a source of sensitive information as well as a high performance tool from which to launch further attacks.

Cyber Attack Techniques

How do data security breaches occur? Some of the incidents are as low tech as stolen or misplaced computer equipment: laptops, hard drives, thumb drives, etc. Reports of stolen laptops surface frequently. Coca-Cola, Inc. recently disclosed that Social Security Numbers, drivers license numbers, and salary information of current and former employees were lost when laptops were stolen from the company ("74,000 Data Records Breached on Stolen Coca-Cola Laptops," 2014). While misplacing a device or falling victim to theft is arguably a result of carelessness, the fact that unencrypted sensitive information was involved falls closer to negligence. Many security breaches involving sensitive information are the result of mishandled data that is stored outside of properly managed and secured systems.

In the case of Target and Neiman Marcus thieves managed to steal credit card data by installing "skimming" hardware or software on point-of-sale computers. Every time a credit card was swiped the software was able to capture customer data stored on the magnetic stripe of the credit cards. This is not an uncommon method of stealing account information, and in fact the industry had been warned of the growing danger of skimmer technology for years (Chickowski, 2011). The scale of the Target and Neiman Marcus attacks point a spotlight at America's antiquated credit card technology. Most other countries have switched to credit cards with embedded chips that store encrypted data, while "almost alone among developed nations, U.S. credit and debit cards have a magnetic stripe that contains all the [unencrypted] financial information necessary to make a purchase" (Dayen, 2014). Upgrading to the more modern "chip and PIN" system requires concurrent

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

investments in new credit cards and readers, and thus most far banks and merchants have declined to make those investments. American consumers even face difficulties using their credit cards in countries that have made the "chip and PIN" upgrades.

Some data breaches occur through what we might popularly think of as hacking, where savvy programmers sit in darkened rooms for hours on end, trying to exploit security weaknesses in software code from remote locations. Some of this malicious code is packaged into so-called "malware" and distributed across the Internet via networks of compromised machines (AKA "Botnets") or through compromised web sites where unsuspecting users inadvertently become infected simply by visiting the site. Exploited weaknesses that become known to the software vendor are usually addressed quickly through the issue of a software patch and it's important for users to keep software up to date when patches are released.

More often, however, data breaches occur through softer "social engineering" paths, where hackers conduct reconnaissance of publicly available information about users. This approach is called targeting and users who have administrative rights on servers or data stores of consequence are prime targets. Hackers may leverage information available about users through social media platforms, which is why it's so important to lock down Facebook profiles because the default settings leave information open for anyone to see. Hackers may use the information they find to exploit relationships, revealing enough to a friend or colleague of their targets to deceive the acquaintances into revealing yet more information that will help hackers gain systems credentials. Administrative assistants of executives may be of particular interest to hackers because the executives have sometimes entrusted them with credentials. In addition to directly stealing sensitive or proprietary information, a primary goal of the hacker is to achieve a toehold on an organization's network from which they can stage other attacks.

A particular form of social engineering is known as phishing. Again, the goal is to gather information but phishing usually employs more automated methods. Phishing attempts may follow the successful theft of personal data, such as the credit card thefts from the department stores described earlier. Once a hacker has what is generally considered protected data they can assume some credibility as they contact the user to gather more information. A phishing attempt often takes the form of a legitimate-looking email that claims to be from an organization or person that is familiar to the targeted user. Spear phishing takes this approach even further with targeted messages that are tailored for specific organizations or even to single individuals. The messages sometimes purport to alert the user to a problem with his/her account and request some action be taken. Sometimes personal or financial information is requested and surprisingly that approach still yields some success with gullible users. Sometimes the user is asked to click a link that is included in the email, leading to an executable program that installs a remote access tool (RAT) or other malicious code such as a key logger that captures all keystrokes (including passwords) on the user's computer. In many cases the user may be unaware that

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

anything unusual has occurred, but once the RAT is installed the hacker gains all privileges assigned to the user.

Don’t Make it Easy

The ever-increasing sophistication and sheer volume of cyberattacks makes any attempts at protecting oneself seem almost fruitless. Personal and institutional data are being stored in so many places, and every time we make another credit card transaction (online or in a restaurant) the danger of losing data increases. Even household appliances like refrigerators and televisions are increasingly connected to cloud-based systems that promise to improve our lives but potentially put us at risk. Innovative new fitness devices like the Nike Training Club for the iPhone or the FitBit store data about us in cloud services. The benefits of being able to share and compare fitness results with a community of athletes are undeniable, but the process puts even more personal data in places where it could be compromised.

The vast majority of librarians will never develop anything close to the cyber security skills needed for protection from all threats, and even with such skills and awareness there are no guarantees of safety. But despair is not an option, and neither is hiding under a rock; the world we find ourselves in is the world in which we must work. Technology is not going away, and few of us would want it to. While we can’t protect ourselves against every intrusive attempt there are some relatively simple things we can do to dramatically improve our security. In many cases, following simple best practices can keep us from being the “path of least resistance” to potential hackers and can help us avoid joining the ever-growing list of victims. Don’t allow your device to become an easy target from which sensitive information is siphoned off or the platform from which hackers launch more serious attacks against your organization’s enterprise systems.

Proper Device Management

Ensuring that updates are applied in a timely manner to all of our devices is one easy step to help protect ourselves. Most vendors release updates to Operating Systems and software on a regular basis – many of which address security problems that the bad guys are already working to exploit. Don’t ignore the automated requests to update software. Password protecting our devices and utilizing encryption are also simple steps in the event that the device falls into the wrong hands. Use that four-digit PIN option for securing your phone should it be lost. Installing and maintaining current anti-virus and anti-malware software and enabling device firewalls when available are additional important steps to help protect the tools we use every day and the information that may be stored on them.

Proper Data Stewardship

Laptops, desktops, tablets, and other client devices that we use for daily communications and web browsing are the least secure location for storing sensitive information. In many breaches that involve these devices the owners either didn’t need the information they were carrying or didn’t even know they had

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

it. Taking the time to handle sensitive information properly – on managed, secure servers or encrypted at rest is essential to helping minimize the risk that you will be responsible for a breach.

Passwords

Passwords have always been one of the most vexing problems in cyber security. The solutions to password security are deceptively simple: create strong passwords, keep them secret, refresh them periodically, and don't use them for multiple applications. But as the number of sites and accounts requiring passwords have multiplied those rules are quickly broken. Nobody can create or remember that many unique passwords.

Often the need to record multiple credentials results in the proverbial sticky note with passwords written on it, and the practice still poses one of the biggest risks to security. We see it all the time: colleagues leave the notes on their computer monitors, on their desks, under their keyboards, or when heightened security measures are really warranted, in a desk drawer. As with all situations that require complex, yet mundane and repetitive action, computers are best tasked to deal with this problem.

Password vault software

Password vault or electronic wallet software represents one of the easiest ways to achieve a sophisticated level of password security for minimal cost. A search on Apple's App Store for the phrase "password vault" currently reveals more than 25 options, ranging from no cost to about fifty dollars. Google's Android App store shows even more results for the same search phrase. These software packages typically allow users to create unique, encrypted passwords for websites that require logins, as well as the option to store other personal information such as driver's licenses or credit cards whose numbers are useful to have if the actual cards are lost. The trick lies in locking it all up with a single, strong password.

What makes a strong password? Unfortunately it tends to be nothing that makes sense to any humans. No words found in a dictionary, no common phrases, nothing that is associated with you personally (dog's name, alma mater, etc), and certainly not the word "password," even if the "a" and the "s" are replaced with "@" and "$." Remember, you're up against hacking algorithms and processing power that can run through millions of variations of common dictionary words and phrases in the time that it takes you to blink. Randomized strings of letters (upper and lowercase), numbers, and symbols are still the best bet, and the longer the better.

Password vault software can generate strong passwords for you, and good software will integrate with web browsers so that usernames and logins can be inserted automatically into websites that require accounts. You can, in fact, create very long passwords that you never see, remember, or handle as you are logging into secure sites because the software takes care of that for you.

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

Good password vault software has to be available at all times to be useful, so look for one that comes in tablet and phone versions as well as a desktop version. It should also use a secure and encrypted cloud synchronization method so that the same login information is available on all your devices. Some software vendors will have their own servers to which the encrypted files are synchronized, others may offer synchronization with common existing services like DropBox or Apple's iCloud. Yes, it may seem counter-intuitive to put your password file in the cloud, but we're always toeing that line between convenience and the kind of ultra-security that makes systems useless. The important thing is that the file that is stored in the cloud is encrypted.

Organizational Responsibility

Organizations that handle and store sensitive information must take their responsibility seriously and dedicate appropriate resources to ensure the security of the information in their care. Organizational leadership must instill a culture of responsible information stewardship and be insistent that cyber security be taken seriously.

It's important for library administrators to develop or adopt policies addressing the management of systems and information and end-user practices, and those policies must be well understood by all in the organization and be appropriately enforced. Organizations must invest in security awareness training for all users and hire and retain properly skilled technical staff with the responsibility and authority to manage systems and networks properly. Additionally, organizations must invest in the proper tools to enable staff to build, manage, and monitor the information infrastructure. Storage systems that provide a secure location for storing and sharing sensitive information are easy to use and are becoming more affordable for organizations to implement. When deployed properly these storage systems provide viable alternatives to carrying sensitive information locally on client devices, significantly reducing the risk of exposure. It is much more economical and efficient to build and maintain a secure environment and instill best practices across an organization than it is to respond to a security breach – just ask Target or Neiman Marcus.

Library administrators have a particular responsibility to ensure that their organizations don't store sensitive information like Social Security Numbers or credit card numbers. Academic libraries are better off partnering with campus IT organizations to take advantage of their firewalls and cyber security expertise.

Credit Cards

Most of us take advantage of online banking conveniences, which also puts us at risk even as it makes our lives much easier. Credit card companies generally conduct very good proactive security practices; their algorithms can reveal when an unusual purchase is made based on previous purchasing behavior and location, and such anomalies will cause the companies to intervene. But credit card companies won't be able to catch every crime. In the ever-escalating arms race of financial fraud savvy hackers devise new methods to defraud their targets. One tactic that has recently gained popularity is for a criminal to charge only small amounts across many accounts, making up in volume and stealth what they might otherwise achieve in large individual crimes that are easier to spot. One of the best ways for a customer to protect himself or herself is to carefully examine monthly online credit card statements. Look at all the charges to verify their legitimacy, and contact the credit card company immediately if you find an illegitimate charge.

What About the NSA?

By now it is obvious to every American that our government gathers data about us. A recent court settlement has allowed the major tech companies like Google, Facebook and Yahoo to reveal the extent (if not the details) of the NSA's requests for data about its customers. "Tens of thousands of accounts associated with customers…have their data turned over to US government authorities every six months" (Ackerman & Rushe, 2014). The National Security Administration's new data center in Utah is capable of storing as much of that data as it wants in "near-bottomless databases…including the complete contents of private emails, cell phone calls, and Google searches" (Bamford, 2012). While the NSA gathers its data through legal means it's likely that their hacking capabilities are second to none and any encryption ability we might have access to wouldn't slow them down very much. We don't mean to imply that the federal government intends to profit from its citizens, but it is worth considering that the government wields an almost unimaginable intelligence force that is largely the result of policies developed following the terrorist attacks of September 11, 2001. Regardless of where you stand, politically, on the NSA's practices it should give you pause to consider just how much personal information you reveal in your everyday "cyber" practices. No system is immune to breach and it can be sobering to imagine the exposure of a reservoir of sensitive information the size of the NSA database, were it ever to be successfully attacked.

Summary

The security of our personal and institutional data and systems should be prominent on our list of concerns. Threats are increasing even as the "Internet of Things" creates a tighter relationship between our physical and virtual worlds, making the ramifications of any data breach more serious. It's not feasible to disconnect from those systems but there are some simple steps we can take and tools we can use to limit the danger and the damage that can occur. Thoughtfulness in all we do online, how we handle our own and others' personal information, and diligence in how we manage our information infrastructure will go a long way towards reducing the risks we all face.

References

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

74,000 Data Records Breached on Stolen Coca-Cola Laptops. (2014, January 27). *Infosecurity Magazine*. Retrieved from http://www.infosecurity-magazine.com/view/36627/74000-data-records-breached-on-stolen-cocacola-laptops-/

Ackerman, S., & Rushe, D. (2014, February 3). Microsoft, Facebook, Google and Yahoo Release US Surveillance Requests. *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests

Baker, S., & Waterman, S. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War* (No. 158). McAfee. Retrieved from http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

Bamford, J. (2012, March 15). The NSA is Building the Country’s Biggest Spy Center (Watch What You Say). *Wired*. Retrieved from http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/

Brynko, B. (2013, June). Cybersecurity: You’ve Been Hacked. *Information Today*, *30*(6), 1–33.

Cheng, A. (2013, December 23). Target’s headaches far from over as consumer perception plunges to 2007 level. *MarketWatch: The Wall Street Journal*. Retrieved from http://blogs.marketwatch.com/behindthestorefront/2013/12/23/targets-headaches-far-from-over/

Chickowski, E. (2011, May 13). Michaels Breach Evidence of Growing POS Skimming Trend. *Dark Reading*. Retrieved from http://www.darkreading.com/attacks-breaches/michaels-breach-evidence-of-growing-pos/229500604

Dayen, D. (2014). Your Credit Card has a Dangerous Flaw that the Banks Refuse to Fix. *New Republic*. Retrieved from http://www.newrepublic.com/article/116236/credit-card-magnetic-stripes-are-putting-you-risk-identity-theft

Johnson, L., Becker, S., Estrada, V., & Freeman, A. (2014). *The NMC Horizon Report: 2014 Higher Education Edition* (No. ISBN 978-0-9897335-5-7). New Media

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu

Consortium. Retrieved from http://www.nmc.org/pdf/2014-nmc-horizon-report-he-EN.pdf

Levin, A. (2013, November 15). Why the Adobe Hack Scares Me - and Why it Should Scare You. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/adam-levin/why-the-adobe-hack-scares_b_4277064.html

Online Trust Alliance. (2014). *2014 Data Protection & Breach Readiness Guide* (p. 39). Retrieved from https://otalliance.org/resources/incident/2014OTADataBreachGuide.pdf

Perez-Pena, R. (2013, July 16). Universities Face a Rising Barrage of Cyberattacks. *New York Times*. Retrieved from http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0

Perlroth, N. (2013, October 29). Adobe Hacking Attack was Bigger than Previously Thought. *New York Times*. Retrieved from http://bits.blogs.nytimes.com/2013/10/29/adobe-online-attack-was-bigger-than-previously-thought/

Summers, B. (2011). *Four Evolving Fraud Threats You Cannot Afford to Ignore* (pp. 1–9). First Data Corporation. Retrieved from http://www.firstdata.com/downloads/thought-leadership/Evolving-Fraud-Threats-WP.pdf

Velasco, S. (2014, January 13). Target, Neiman Marcus Face Data Breaches. Now, Others? *Christian Science Monitor*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=93724036&site=ehost-live

Address correspondence to Kenning Arlitsch, Dean of the Library, Montana State University,
P.O. Box 173320, Bozeman, MT 59717-3320, USA. E-mail: kenning.arlitsch@montana.edu