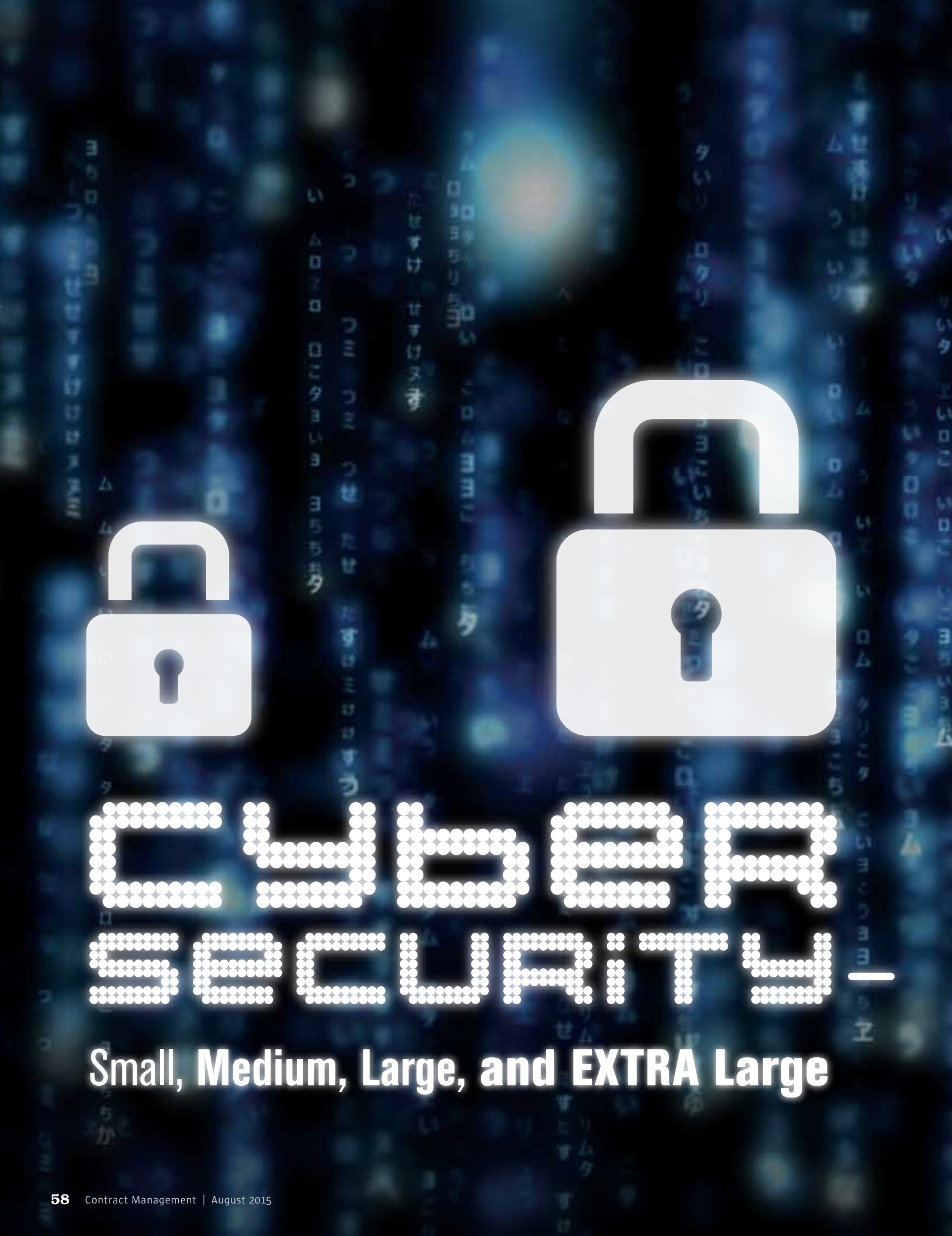
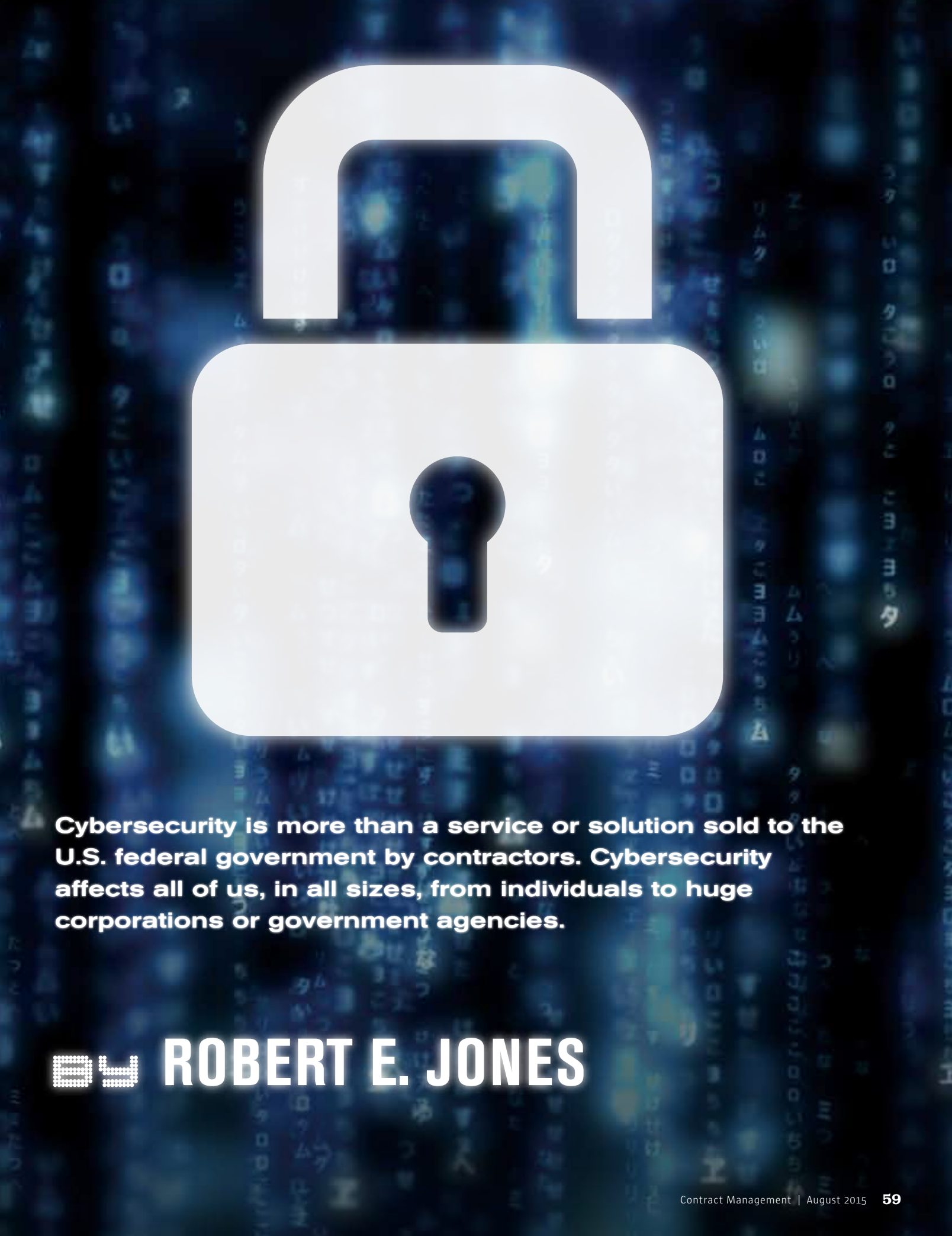


Cyber Security—

Small, **Medium, Large, and EXTRA Large**



Cybersecurity is more than a service or solution sold to the U.S. federal government by contractors. Cybersecurity affects all of us, in all sizes, from individuals to huge corporations or government agencies.

BY ROBERT E. JONES

Cyber terrorism has been called the biggest threat to America`s economic security.[1]

From individuals to global enterprises, cyber security threats are real for all of us.

The Target, Home Depot, and Sony breaches[2] are well-known to many of us because of the substantial news coverage and were likely targets because of the amount of data, the deep pockets, and the impactful message. What may be a larger risk are all of the small- and medium-sized businesses who have not adequately secured their data.

What is Cyber Security?

The Department of Homeland Security (DHS) defines *cybersecurity* as "the protection of computers and computer systems against unauthorized attacks or intrusion."[3]

What is a Hack or Breach?

Simply stated, a *hack* or *breach* is an unauthorized access to an account, network, or data, and/or the theft or use of that data in an unauthorized manner.

What is at Stake?

- E-mail;
- Social media (e.g., Facebook, LinkedIn, Twitter, etc.);
- Cloud storage (e.g., Google Drive, Office 365, Box, Dropbox, etc.);
- Online accounts (e.g., banks, Amazon, utilities, etc.);
- Mobile devices;
- Corporate networks;
- Intellectual property;
- Proprietary data;
- Personally identifiable data;
- Classified military data; and/or
- Homeland security.

Who is Vulnerable and Why are They Targeted?

Individuals (Small)

Identify theft has been around for years. People once stole the carbon copies of credit card receipts, mail, and other paper items as a form of fraud. With a more paperless and more digital society, criminals changed their tactics. If you're an adult and were alive in the last few decades, you have an online presence whether you created it or not. What you did not create, a company probably created for you in maintaining their own records. If you have an e-mail account and transact any business online, you definitely have a presence. So what? From a global perspective, one individual's theft of identity may not trigger any alarms. From a personal perspective, it likely means some embarrassing spam to your family or friends, a police report for credit card fraud, and possibly several hours sorting through the mess. A good friend of mine had her identity stolen in the form of a fraudulent tax return and refund that forced her to file a police report, notify the three major credit bureaus, and make special filings with the IRS and FBI because of the specific nature of the event.

Many of us know the risks as individuals: A stolen credit card number, a hacked e-mail or social media account, or compromised health data. I suspect that many of us have either had our own e-mail account hacked or directly know someone who has. Ever notice those crazy spam messages from your family and friends in your junk folder? Those are most likely the result of a hacker. Childs play, maybe, but consider the amount of information many of us send or store in e-mail. Further consider that these hackers are just practicing and using the same techniques on businesses and governments of all sizes.

Small and Medium Businesses (Medium)

➢ *The Bigger Problem: Individuals as Employees*

While individual cybersecurity is a problem, the bigger looming problem that's difficult to quantify is the amount of corporate network access and business data in the hands of employees. Let's start with mixing the use of personal and business e-mail accounts. A good example would be Hillary Clinton while she served as secretary of state. I'm sure she would agree it's a conflict of interest, in the least, or "one great big mistake," as Sen. Chuck Grassley stated.[4] Not only is it unprofessional to send or receive work messages through your personal e-mail account, but it's a conflict of interest and a breach of corporate policy for many organizations. Not to mention, it's confusing to track and maintain. As a business owner or manager, you should be very concerned about what your employees send and receive through e-mail—yours and theirs. The joke for many years was literally about the sharing of jokes clogging up corporate e-mail servers. Online pornography and gambling presented new issues for businesses. Now, the concern is keeping the proper data inside the network and unauthorized users outside of the network.

The real problem is that your employees may not be adequately separating their work and personal lives. Do they work from home and access corporate networks or customer and supplier portals from their personal computers? Where are those passwords stored? In a browser? In an Excel file? How are they transferring files and other data for use offsite? How many of us have e-mailed ourselves a file to work on at home?

Target, Home Depot, and Sony (Large)

Even with large departments committed to cybersecurity, look at the damage to reputations and the cost to companies to clean up these breaches. Not only are there attorney fees, but the internal cost of staff, paying for credit monitoring services for those whose data were compromised, fees for reputation management and public relations firms, and the potential fines. For large companies, a single data breach can cost millions of dollars. Sony's hack is reported to have cost $15 million.[5]

Governments, Defense (Extra Large)

The U.S. Department of Defense (DOD) recognizes cybersecurity or cyberwarfare as the biggest threat to our nation and recently released new guidelines to achieve dominant capabilities through technical excellence and innovation as part of Better Buying Power 3.0.[6] For many years, wars were fought on the ground—in hand-to-hand combat. Remember Col. William Prescott's famous line during the Battle of Bunker Hill? "Don't shoot until you see the whites of their eyes." Later, warfare became more complex with the introduction of airplanes, ships, and submarines. Recent years have added drones or unmanned aircraft, and now we have cyber criminals—hackers working around the world to bring down any and all of our systems, including communications and electrical grids.

Tools You Can Use

Password Management

The use of strong passwords and password management is a daunting task for many individuals. With multiple online accounts to run our personal lives, keeping track of everything is a task in itself. What about all of the online accounts to run our businesses? As previously stated, small- and medium-sized businesses are extra vulnerable as employees often "wear many hats" and have access to a number of personal and corporate resources. The key for the business owner is ensuring that employees maintain a clear separation between their personal and professional online lives.

➢ *Recommendation*

Large organizations often have enough delegation and segregation of duties and access to robust tools for network security and password storage. For individuals, I recommend LastPass[7] or KeePass.[8] Both are encrypted and include password generators that create unique passwords (e.g., "f8Dkl@i*sm0") to further obscure your online presence. LastPass is also an excellent solution for small businesses. For professionals, create one account for home and one for business. Better yet, small business owners can create enterprise accounts allowing them to recover or revoke access as necessary. Onelogin[9] and ManageEngine[10] provide services for enterprise organizations from a few employees to several thousand.

Wi-fi and Bluetooth

That free wi-fi at your local coffee shop, pub, or library is often not secure. One quick way to tell is the use of a password. If no password is required to access the wi-fi hotspot, then it's not secured. There are similar concerns with the Bluetooth on your laptop and mobile devices—just another way for a hacker to access your system and steal data.

➢ *Recommendation*

Keep wi-fi and Bluetooth turned off until you need them, know the device/person/network to which you are connecting, and always use a secure network. If you travel regularly for work, consider using a corporate VPN (supplied by your IT department) or a service such as Avast SecureLine VPN.[11]

Mobile Devices

Phones and tablets are vulnerable to hackers, viruses, trojans, and security breaches, too. Ever think about all of those apps on your smart phone? Do you know what data they access and how or where it's stored?

➢ *Recommendation*

Use a PIN/passcode on your device, be able to remotely wipe the device if it is ever lost or stolen, and install mobile security such as Avast Mobile[12] (for Android) or Avira[13] (for iOS).

E-mail Accounts

Most professionals I know manage any number of e-mail accounts. Many people maintain multiple personal accounts—one for bills and important information, one for Facebook and other social media, and one for family and friends. In business, we may maintain multiple e-mail accounts because of our job duties or involvement in professional or volunteer organizations. The key is keeping them separated. Keep in mind that

employers of any size can read your e-mail on their servers. Forget hackers—do you want people at work digging through your personal life?

➢ *Recommendation*

Do not send personal e-mail through your work or professional account and vice-versa. The former can be embarrassing and the latter is unprofessional, potentially unethical or illegal, and obscures the ability of the organization to properly archive data for legal proceedings. E-mail accounts are free and easy to establish. You probably have some freebies with your Internet service provider and you can sign-up with Gmail, Hotmail, Yahoo, or Outlook.

Cloud Storage Accounts

As with e-mail accounts, most professionals I know manage at least one personal storage service such as DropBox, Google Drive, Box, or Office 365. The same is true with many small businesses and professional or volunteer services. Collaboration is king in 2015, so we share all kinds of documents and data with other members of our teams.

I love cloud services and swear by the ones I use. Having all of life's necessary documents backed-up, encrypted, and available from any device is very important to me. The problem for businesses may be the cloud services they are using or the fact that employees are storing corporate data on personal servers.

➢ *Recommendation*

Do not store personal documents on a business or team server and vice-versa. The former can be embarrassing and the latter is unprofessional, potentially unethical or illegal, and obscures the ability of the organization to properly archive data for legal proceedings. Again, there are a number of free or inexpensive services with tiered plans to meet the needs of individuals, groups, teams, and enterprises.

Encryption and Data Files

Encryption is the common denominator in all of these tools. Unique passwords stored in encrypted vaults used to access encrypted data via an encrypted VPN makes it virtually impossible for someone to intercept or decipher information. Ever notice the "https://" (with the "s") in the address bar of your Internet browser? That means you have an encrypted connection to the server providing the data.

You can also encrypt the contents of your hard drive or cloud storage so that all of the individual files are encrypted. Even if someone stole your laptop, they would need the password to the encryption program to access any data. Companies such as SertintyOne[14] now provide software that utilizes advanced authentication methods to protect data independent of operating systems.

Multi-Factor Authentication

Once reserved for classified data and other sensitive items such as corporate bank accounts, multi-factor authentication is available to everyone for nearly every type of account. Multi-factor authentication comes in three main forms:

- Digital certificate—Software and/or hardware token such as IdenTrust.[15]
- One-time password generator—Hardware token such as RSA SecurID[16] or mobile app such as Google Authenticator.[17]
- Verification code via text or e-mail—Set-up through that specific online account.

Multi-factor authentication works by requiring an extra layer of credentials to access a network or account. The user enters their user ID, password, and a third unique code, password, or digital certificate that authenticates or verifies his or her identity. The effectiveness comes in two ways: You have to be verified in some manner to obtain the third-party app, token, or certificate and you must have that physical item and the user ID and password (presumably in your brain) to gain access to a resource. By requiring all three pieces of information, one of which changes constantly based on an algorithm, it's more difficult for hackers to gain unauthorized access.

Special Considerations for Government Contractors

Export-controlled technical data is governed by the *Export Administration Regulations* (*EAR*) and *International Traffic in Arms Regulations* (*ITAR*). The latter is often more applicable to government contractors (especially defense contractors) due to the advanced technical nature of the products and services they provide. Technical data transmission and storage are governed by the *ITAR* and the use of e-mail and cloud storage are discouraged due to the fact that files can be transferred through or stored on servers in other countries creating a "deemed export," which are when technical data is disclosed or merely accessible to an unlicensed or unauthorized foreign person or entity.

On November 18, 2013, DOD issued a final rule amending the *Defense Federal Acquisition Regulation Supplement* (*DFARS*) to add a new subpart and contract clause (DFARS 252.204-7012) associated with safeguarding unclassified controlled technical information.[18] The new rule requires that contractors with "controlled technical information" resident on or passing through their information systems use a minimum set of protective measures and security controls to safeguard the data. In addition, contractors will be required to notify DOD of any cybersecurity intrusions or incidents that have an effect on controlled technical information or that allow unauthorized access to the information system on which the unclassified controlled technical information is stored. The rule further mandates these requirements also be flowed down to the contractor's subcontractors and vendors, even in the commercial setting.[19]

Lastly, remember that classified data must be stored on a separate system approved by the Defense Security Service Office of Designated Approving Authority[20] and is governed by the *National Industrial Security Program Operating Manual* (*NISPOM*). **CM**

ABOUT THE AUTHOR

ROBERT E. JONES, CFCM, CCCM, FELLOW, is the president of Left Brain Professionals Inc., where he supports clients on a number of government contract and accounting projects, including incurred cost proposals, commercial item determinations, and accounting system design. He holds a BA in accounting from Queens University of Charlotte and an MS in accountancy from the College of Charleston. He is pursuing his CPCM and CPA, and currently serves as the president of the Central Ohio Chapter of NCMA.

Send comments about this article to cm@ncmahq.org.

ENDNOTES

1. *See* **www.cnbc.com/id/100460895**.
2. *See* S. Poremba, "2014 Cyber Security News Was Dominated by the Sony Hack Scandal and Retail Data Breaches," *Forbes* (December 31, 2014), *available at* **www.forbes.com/sites/sungardas/2014/12/31/2014-cyber-security-news-was-dominated-by-the-sony-hack-scandal-and-retail-data-breaches/**.
3. DHS, "Cybersecurity 101," *available at* **www.dhs.gov/sites/default/files/publications/cybersecurity-101_4.pdf.**
4. D. Montenaro, National Public Radio (April 2, 2015), *available at* **www.npr.org/blogs/itsallpolitics/2015/04/02/396823014/fact-check-hillary-clinton-those-emails-and-the-law.**
5. M. Shilling, "Cyber Hack Revealed as Costing 15 Million as Sony Inreases, Forecast Results," *Variety* (March 17, 2015), *available at* **http://variety.com/2015/biz/asia/cyber-hack-revealed-as-costing-15-million-as-sony-increases-forecast-results-1201454231/.**
6. F. Kendall, "Implementation Directive for Better Buying Power 3.0," Defense Acquisition University, *available at* **http://bbp.dau.mil/docs/BBP3.0ImplementationGuidanceMemorandumforRelease.pdf.**
7. *See* **www.lastpass.com.**
8. *See* **http://keepass.info/.**
9. *See* **www.onelogin.com.**
10. *See* **www.manageengine.com.**
11. *See* **www.avast.com/en-us/secureline-vpn.**
12. *See* **www.avast.com/en-us/free-mobile-security.**
13. *See* **www.avira.com/en/free-antivirus-ios.**
14. *See* **www.sertintyone.com.**
15. *See* **http://identrust.com/.**
16. *See* www.emc.com/security/rsa-securid/rsa-securid-hardware-tokens.htm.
17. *See* **https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8.**
18. *DFARS* Case 2011-D039.
19. DFARS 252.204-7012.
20. *See* "Certification and Accreditation and Oversight and Management of Cleared Contractor's Computer Systems," Defense Security Service, *available at* **www.dss.mil/isp/odaa/odaa.html**.