ARTICLE COURTESY OF LEXICON SYSTEMS, LLC • +1 281 280 8106 • lexicon-systems.com

# Cybersecurity: A Global Issue

Information security is a growing concern for individuals, the public sector, and private sector. We want the ability to easily access and share information—instantaneously—from large databases over the Internet, yet more and more of us are using untethered smartphones, tablets, and laptops to do so. And now we even have "smart" automobiles, home security systems, and appliances that transmit data over the Internet. Information-sharing is critical in our personal and business lives. So how can we better protect identities, data, and devices?

Information technology (IT) advances quickly, leaving individuals, businesses, and the global economy with the task of protecting systems and information. Those with aging computer systems that do not employ the latest security measures can be the most vulnerable to risk.

## High-Profile Hacking

Yesterday's hacker was a teenager in a basement, gulping down energy drinks and hacking for the thrill of it. Today's hacker is a sophisticated professional, often working for a criminal organization or rogue city-state for highly profitable data theft.

Recent high-profile security breaches include the Target customer credit card and Sony Pictures Entertainment e-mails hacks in 2014 and the U.S. military social network and Anthem health

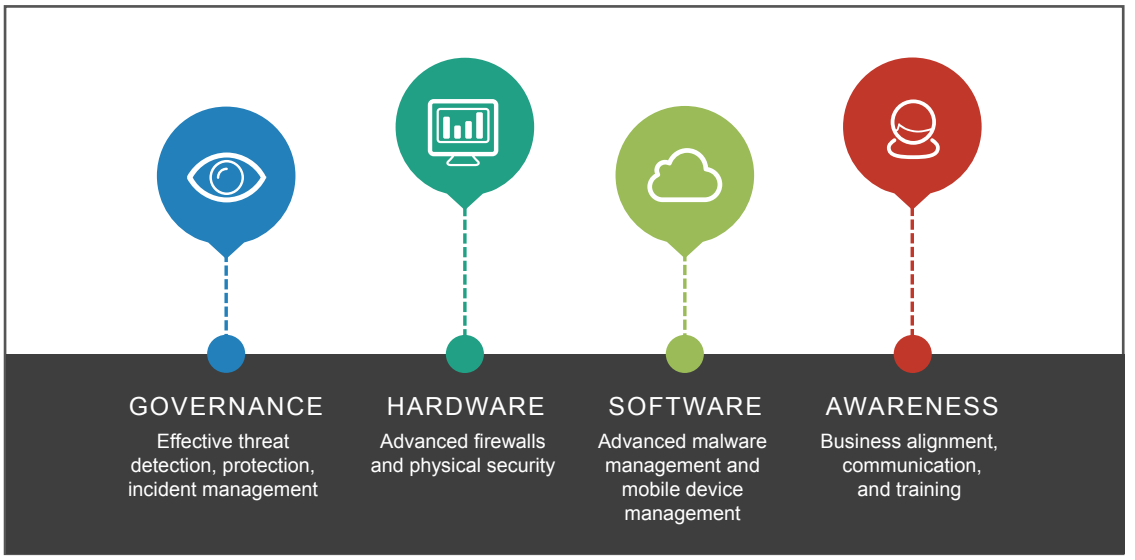



Figure 1. Cybersecurity strategy.

insurance information breach in early 2015. These incidents show how sophisticated and far-reaching cyber attacks can be. And these are just the ones that made the headlines!

The Software Innovation Division at the Defense Advanced Research Projects Agency (DARPA), headed by Dan Kaufman, is a team of experts who are trying to find new ways to fight cyber crime. Half of Kaufman's division's mission is to stay ahead of catastrophic events.[1] DARPA, the U.S. Department of Defense agency that developed the first network to use Internet Protocols in the 1960s, must now find a way to secure the Internet.

## New Data Security Risks

Cybersecurity was on the agenda at the World Economic Forum Annual Meeting in Davos, Switzerland this past January. A week later, the President of the United States spoke about cybersecurity in his State of the Union Address and called for new, bipartisan legislation: "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families… we're making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism."[2]

With personal, financial, and competitive data at stake, individuals and organizations should have an expectation of data privacy. Newer information technologies like the Internet of Things, social networking, and mobile devices offer a wealth of features and functions, accompanied by new data security risks.[3]

### The Internet of Things

The Internet of Things allows Internet-connected appliances, cars, and health monitors to use and share data. At work, for example, your inkjet printer sends a message to the supplier when an ink cartridge is low on ink. A new cartridge then arrives automatically within a business day or two. At home, your refrigerator knows when the water filter needs replacing, and you automatically receive a new filter, saving you a trip to the hardware or big box store. On the road, if you lock yourself out of your car, you can call a toll-free number to have the car unlocked remotely.

Here's the tradeoff: industry provides new functionality, and consumers increasingly disclose personal information. Consumers must be proactive when dealing with Internet-connected devices and personal information. However, few people read privacy policies when providing information via the Internet.[4]

### Social Networking

Social networking, Web-based e-mail, instant messaging, peer-to-peer, and file transfer applications allow people to share information quickly and easily across multiple platforms. At the same time, these applications open the door for "social

'The number of [cyber] attacks is dramatically increasing; the sophistication of attacks is increasing.'

—Dan Kaufman, Director, Software Innovation, DARPA[1]

engineering," where an attacker impersonates a friend or colleague and entices a user to perform an unsafe act like click on a malicious link.

### Mobile Devices and Mobile Banking

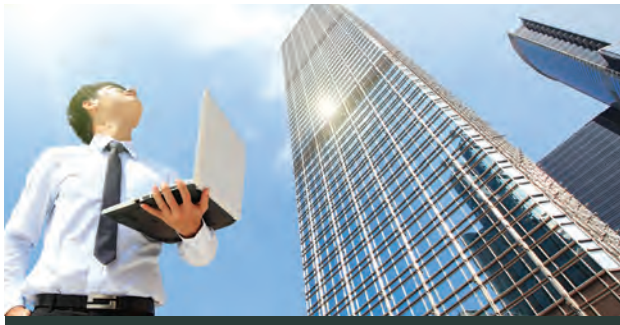
People in general are comfortable with their mobile devices and rarely think twice about downloading a new app, especially if it is free. However, this opens the door for inadvertent sharing of sensitive information. Smartphones and tablets allow data sharing in the enterprise, ranging from customer lists in customer relationship management (CRM) apps to e-mail and content management systems to enterprise environment, health, and safety (EH&S) management information systems.

Mobile banking provides easy-to-use, on-the-go capabilities; take a photo of a check with your phone, and deposit it for instant gratification. Mobile payment systems like Square are a boon for small businesses and have moved to larger enterprises. The recent introduction of Apple Pay has credit card companies, businesses, and consumers clamoring for the service, although currently only people with an iPhone 6 can use it.

### Next-Gen Cybersecurity

Traditional network security measures like firewalls, intrusion protection, proxies, and simple passwords are no match for the 21st century hacker. In *Cybersecurity for Dummies*,[4] Lawrence Miller warns that you must assume that you will experience a network breach at some point, no matter how good your policies, and plan accordingly.

Next-generation security requires a solid, well-thought-out strategy that addresses hardware, software, and governance.[5] I would add a fourth, human element to the mix: awareness is critical to successful implementation of the strategy (see Figure 1).



## What You Can Do to Protect Your Data

**Nearly one quarter (23%) of employees believe that data security is not their responsibility.[6] If you think that data security is someone else's problem, think again. Here are 10 ways you can contribute to the cybersecurity effort:**

1. **Set your computer for automatic software updates.**
2. **Install protective software.**
3. **Choose strong passwords.**
4. **Backup your data. And back it up again.**
5. **Control access to your machine.**
6. **Use e-mail and the Internet safely.**
7. **Use secure connections.**
8. **Protect sensitive data.**
9. **Use desktop firewalls.**
10. **Stay informed.**

Cybersecurity is a growing global concern, and each of us must play a role in addressing potential threats. The pervasiveness of the Internet of Things, social and collaboration tools, mobile devices, and mobile payment technologies can leave sensitive data vulnerable. The human factor is critical to meeting an expectation of data privacy and security. em


### References

1. CBS News, *60 Minutes*, "DARPA: Nobody's Safe on the Internet," February 8, 2015. See http://www.cbsnews.com/news/darpa-dan-kaufman-internet-security-60-minutes/.
2. The White House, *Remarks by the President in State of the Union Address, January 20, 2015*. See http://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015.
3. Homeland Security News Wire, *Emergence of the Internet of Things Significantly Weakens Privacy Protection*, February 5, 2015. See http://www.homelandsecuritynewswire.com/dr20150205-emergence-of-the-internet-of-things-significantly-weakens-privacy-protection.
4. Miller, L.C. *Cybersecurity for Dummies, Palo Alto Networks Edition*; John Wiley & Sons Inc.: Hoboken, 2014.
5. Massachusetts Institute of Technology, Information Systems & Technology, *Top Ten Safe Computing Tips*. See https://ist.mit.edu/security/tips.
6. McDonald, C. "Data Security Is Not Their Responsibility, Say 23% of Employees;" *Computer Weekly*, January 30, 2014. See http://www.computerweekly.com/news/2240213483/Data-security-is-not-their-responsibility-say-23-of-employees.