National Cyber Security Awareness Month in October 2014 saw JPMorgan Chase announce that criminals had accessed more than 76 million of its customer records. The ironically timed crime was one of the largest data breaches ever, but it still wasn’t a record. Adobe Systems had lost nearly twice that many—130 million records—in 2013.

With startling regularity, we are treated to news stories of data breaches at major corporations. It seems as if every day brings a new worry for your cyber security. Were those home goods worth my credit card information being stolen? How much do I love being able to Photoshop® funny cats into all of my holiday photos? Enough to have my personal information compromised? Is this new drill purchased from the hardware store worth the potential hassle? As they seem to be getting more and more frequent, data breaches can certainly turn anyone into a hacking hypochondriac, all with good reason.

Additionally, all of these stories vary in detail, but nearly every one is summarized with a line that is depressingly familiar: “one of the largest corporate data breaches ever reported.”
Criminal hacking is the new normal in the cyber world. Cybercrime is a big business, so we can expect to see more and more miscreants trying to capitalize on the vulnerabilities in our information systems. Sophisticated individuals, criminal organizations, and foreign governments drive much of the activity we see.

And lately there is a new trend. In September 2014, Dairy Queen announced that 395 of its stores were robbed of payment card information by a malware program called Backoff. Dairy Queen is itself a large corporation, but individual locations are independently owned and operated. To its credit, International Dairy Queen Inc. worked closely with franchisees to find and eradicate the malware. Was the Dairy Queen breach an attempt by criminals to gain access to a large corporate information system through the back door of local franchises? It is notable that the attackers accessed the Dairy Queen systems after obtaining account credentials from a third-party vendor. The hackers were definitely trying to sidestep Dairy Queen’s security systems.

Increasingly, organizations are finding it difficult to harden their systems against intrusions. In today’s world, doing business means opening your information system to customers and suppliers, and the company that gives you the best deal on, say, cleaning services may not be the company that has the best cyber security. Because so much of modern commerce is networked, criminals are increasingly able to attack large corporations by infiltrating the small- to mid-sized companies they do business with. Once in, malware can spread like a disease if it is left undetected.

The franchise system may be particularly vulnerable because franchisees are often responsible for their own security, without much guidance or oversight from corporate. Reporting security incidents is not always required, and there may be no response plan in place, allowing malware and breaches to persist without detection.
It may be the case that large corporate data breaches are just the tip of the iceberg. Ponemon Institute, which annually surveys the cost of data breaches globally, doesn’t even count the headline-making major breaches. It considers them too rare to be instructive! The cases used to compile the 2014 Cost of Data Breach Study, which was performed by Ponemon Institute and sponsored by IBM, are events involving fewer than 100,000 records. The average incident in the report was based on the loss of only 29,087 records.

**Ponemon Institute calculates your probability of incurring a material data breach in the next two years to be about 19 percent, which is nearly one in five.**

And, while we say “only 29,087 records,” we must hasten to add that Ponemon Institute calculated the average cost of a data breach to be $201 per record, giving the average data breach a cost of nearly $6 million to its corporate victim.

The criminals attempting to breach corporate systems are both relentless and increasingly well capitalized. Their sheer numbers and persistence render them dangerous. They constantly probe potential corporate victims, and being a small and relatively unknown organization is no longer a protection against them. In September 2014, North Dakota State College of Science said it had found malware on computer servers that contained student and employee names, Social Security numbers, and mailing addresses. There is no evidence the records were actually accessed, but 15,000 people had to be notified of the possibility.

When criminals go after North Dakota State College of Science, there is probably no organization that is safe. In other words, if your organization has not yet experienced a data breach, it probably will. Ponemon Institute calculates your probability of incurring a material data breach in the next two years to be about 19 percent, which is nearly one in five.

What are the costs of a data breach? The costs tend to vary from industry to industry, but Ponemon Institute summarized its calculation method in the 2014 report this way:

The total cost of a breach, according to the Cost of Data Breach Study, is on the rise after a brief period of decline. Much of the rise is due not to increasing repair or investigation costs, but to increasing customer departures resulting from breaches. This year’s report found that organizations that experience data breaches have a 15 percent increase in customer turnover. The increasing publicity surrounding these events has heightened public awareness and sensitized people to their own vulnerabilities. Customers are often unforgiving when an organization appears to put their personal information at risk.

While the first-order costs of a data breach consist of the expenses required by investigation, repair, and making injured customers whole, the second-order costs are the expenses of the public relations and advertising required to convince the world at large it can trust your organization. You must add to this the expenses of acquiring customers to replace those who abandon you. The second-order costs are higher than the first-order costs, and they are rising quickly.
The information systems industry has been tirelessly fighting cybercrime with technology. There are seven broad categories of technology designed to protect corporate information resources, which are as follows.

**ACCESS CONTROL MANAGEMENT**
Access control management is the most basic security technology, since the whole point of security is to prevent access for those who should not have it. An access control management system typically includes a method for challenging the identity of a user and then providing only the rights (read, write, and/or edit) the user is entitled to. The best of them are capable of measuring the strength of a new password even as the user composes it. But even the strongest passwords may be vulnerable to sophisticated password cracking software.

**ANTIVIRUS**
Antivirus systems prevent access to the information system, not by users, but by malicious or rogue software. Viruses were originally programs that attached themselves to other programs or boot disk sectors, but today, the term more commonly covers worms or Trojan horse programs. Antivirus systems are programmed to recognize known viruses or to monitor the system for activities that usually indicate a virus. The best of them get frequent automatic updates (weekly or better) to their databases of virus signatures, but this requires a vendor that maintains a substantial research effort to track new viruses.

**FIREWALLS**
Firewalls insulate computers or networks from the Internet or from other networks. Desktop systems often include software-based firewalls designed to prevent intrusion from the Internet. Firewalls can be hardware-based as well, and they often perform routing or server functions in addition to protection. Most security experts regard a firewall as necessary, but note they are not sufficient protection systems.

**INTRUSION DETECTION & ANALYSIS SYSTEM**
Intrusion detection and analysis systems detect anomalous behavior in a computer or network and report it or act to prevent or contain it. Intrusion detection systems (IDSe) are programmed to recognize known bad traffic or to monitor a system for activities that indicate it. Their principal limitation, like that of antivirus programs, is in keeping up with the increase in bad traffic. They need to be updated constantly, and as their databases grow to accommodate new signatures, performance can suffer.
Emerging technologies in the hands of bad actors have increased the need for new solutions and bigger budgets. The Internet of Things (IoT) has added a layer of complexity to the problem. There are now numerous access points to protect (think moving from a two-door house to a house with 20 doors). While an increasingly interconnected world is a net positive, there are those with malicious intent ready to capitalize on our failure to keep pace with the changing ways in which we do business.

The key is striking a balance between technological and human solutions. No system alone can protect itself from cybercrime without the management and oversight of skilled workers. Likewise, information security professionals need to rely on their first line of defense, technology, to identify breaches as they happen. The key is to close the lag time between when a security system identifies a vulnerability and when security professionals act. In the case of the famous Target breach of 2013, anti-intrusion software alerted staff a number of times. These alerts went unanswered. As a result, over 100 million individual records were stolen.

**AUDIT DATA REDUCTION**

Audit data reduction systems reduce the amount of audit data an IDS must process, increasing its speed and effectiveness. This is one of the leading-edge areas of security technology.

**VIRTUAL PRIVATE NETWORKS**

Virtual private networks (VPNs) are designed to emulate private networks (as if on private leased lines) on public networks using software. A VPN is usually not intended to be a security system, but it usually provides encryption in order to protect the data it sends over public networks. In addition, it can include logging capabilities that can be used to report attacks. VPNs may not require as much vigilance as public network connections, but users still should apply basic security practices (see the sidebar for more).

**VULNERABILITY SCANNING SYSTEMS**

Vulnerability scanning systems scan and test networks for weak spots. They don’t necessarily provide protection; they just provide information that should inform protection efforts.

Some of these technologies have advanced significantly over the past few years, and many are remarkably sophisticated. The thing they all have in common, however, is that they are only the first line of defense in protecting information systems. You can’t simply install them and expect them to protect you indefinitely. Someone has to maintain them, someone has to monitor them, and everyone in the organization has to recognize their limitations.
The front-line people in the security war are the IT security professionals.

Security professionals have, traditionally, accounted for a smaller percentage of overall IT staff than one might expect. There are a number of functions in an IT department and keeping information safe is not generally the primary focus.

The proportion of security professionals to total IT staff, of course, varies by industry. Generally speaking, the more confidential information an organization has to protect, the higher the proportion of staff dedicated to information security. In banking or healthcare, it is much more important to protect your information than some other industries. Not to say that cybercrime can’t affect any number of industries, but the most at-risk are those that deal heavily in data.

The one silver lining of the headline-making crimes of recent years is that they have begun to drive change in how we think about security. More resources are dedicated to ensuring the safety of our information systems today than yesterday, and more will be applied tomorrow than today. For example, JPMorgan Chase has committed to investing $250 million annually in corporate information security. By year’s end, they anticipate employing 1,000 professionals dedicated to preventing another breach from occurring. As these attacks become more commonplace and more costly to a company’s bottom line, corporate executives are forced to take notice and commit more resources to security.

A critical step, however, will be the development of a dialogue between IT management and the C-suite. For too long, IT has
operated in a silo, removed from conversations regarding greater business initiatives. As the costs of this negligence have appeared in the headlines, decision makers are beginning to see the intrinsic value of data and the need to protect it. In a world of diminishing resources, information security is beginning to get the attention it deserves.

Success lies in aligning a company’s business objectives with their security operations. Understanding that continued business growth is now tied directly to securing an organization’s information systems is a critical step in moving towards a safer, more secure world. Every employee must have a stake in security and understand the need to be vigilant.

IT security professionals face a host of complex issues on a day-to-day basis. Maintaining up-to-date certifications can ensure that professionals are equipped with the knowledge necessary to combat persistent and growing threats. Just as technology must evolve, so must our understanding of the methods used by hackers. Facilitating an open dialogue regarding threats and learning from the mistakes of other organizations quickly can help to prevent future security incidents.

Professional networking, then, is critically important to IT security professionals. Organizations need to allow them the flexibility to join organizations of their peers and to communicate with their counterparts. This is not an area that should be covered by policies on trade secrets. An organization that tries to treat security as a competitive edge may find itself without the lines of communication needed to request help when it is attacked. Failing to cooperate with other organizations when it comes to security is bound to backfire.

As our world becomes increasingly complex, our solutions to data vulnerabilities must gain complexity as well. This requires a partnership between threat detection technologies and the security professionals that monitor them. The faster we can close the loop when threats occur, the more we can mitigate the damage.

It goes without saying you should implement the best, most reliable security technology you can afford, and there are lots of resources on the Internet to help you do that. Much of the best-regarded software is open source, which usually means it is inexpensive to acquire and that it has a worldwide community committed to keeping it up to date.

But technology will never offer complete protection. You must account for the human element, and that means combining a mixture of training and corporate culture to the problem.
The security field offers a number of certifications for security professionals. Logical Operations, for example, has developed CyberSec First Responder: Threat Detection and Response (CFR), a course designed specifically as a proactive mitigation response to security risks through a sound security posture. This five-day lab-intensive certification course was developed by industry leaders and is based on comprehensive customer feedback pertaining to security training. CyberSec First Responder allows organizations to develop the skills necessary to create an information assurance lifecycle process and enforce an understanding of all aspects of network security, from designing a secure infrastructure to auditing.

The SCYBER course helps learners gain competence in four areas of network security:
• Monitoring security events
• Configuring and tuning security event detection and alarming
• Analyzing traffic for security threats
• Responding appropriately to security incidents

In other words, both the SCYBER and CyberSec First Responder courses intend to shift the element of surprise back from the criminals to the corporations. Those who know how to monitor security events and detect bad traffic can guard against it. It is a new kind of war, but those on the front lines can learn a lot from the old kind of war. You wouldn’t rely entirely on fortifications to protect a sensitive position in the field; you would post sentries and lookouts. The same goes for computer systems. It is not enough to harden and fortify the system. You have to watch over it as well so you are not taken by surprise.

The act of training a security professional in your organization is a win-win in that it provides protection for the organization’s information assets and a secure career path for employees. For example, once an employee gains the Cisco CCNA® (Cisco Certified Network Associate) Security certification, he or she is eligible to continue training for Cisco CCNP® (Cisco Certified Network Professional) Security certification and Cisco CCIE® (Cisco Certified Internetwork Expert) Security certification, leading to network security engineer job roles.

There will always be a demand for IT security professionals. Certification programs guarantee the credentials and basic skills of these professionals, ensuring the future of anyone who chooses security as a career path.
The security field offers a number of certifications for security professionals. Logical Operations, for example, has developed CyberSec First Responder: Threat Detection and Response (CFR), a course designed specifically as a proactive mitigation response to security risks through a sound security posture. This five-day lab-intensive certification course was developed by industry leaders and is based on comprehensive customer feedback pertaining to security training. CyberSec First Responder allows organizations to develop the skills necessary to create an information assurance lifecycle process and enforce an understanding of all aspects of network security, from designing a secure infrastructure to auditing.

The CyberSec First Responder course focuses on the following skills necessary to secure an organization’s network:

- Assessing security risk and posture
- Analyzing threats
- Designing secure environments
- Collecting real-time security intel
- Responding to and investigating incidents
- Auditing to ensure secure environments

In addition to CyberSec First Responder, Logical Operations also offers the Securing Cisco® Networks with Threat Detection and Analysis (SCYBER) course toward certification as a Cybersecurity Specialist.

This five-day lab-intensive training course prepares individuals with the standard CCNA® (Cisco Certified Network Associate) and basic Cisco IOS® software switch and router configuration skills to take the Cisco Cybersecurity Specialist certification exam.

While it is important for an organization to commit to the development of security specialists in the organization, it is just as important to raise security awareness throughout the organization. Security needs to become every employee’s concern. As major security breaches become more prevalent, it is likely that employees will become more vigilant on their own. But this is not something that can be left to chance, and you are never going to eliminate user error altogether.

**Ultimately, every employee needs to understand that securing their organization’s information systems starts and ends with them.**

The best way organizations can work to mitigate the risk is to have an open conversation with employees about the importance of data security. Communicate the need for sound security practices (the minimum practices are described in the sidebar), and share the ways in which it can affect them individually. In many organizations, a quarterly loss in the millions as a result of a data breach may eliminate salary increases, at least temporarily. Everybody in the organization can understand that.

Getting back to basics can go a long way to ensuring better stewardship of an organization’s data. Ensure that all employees are aware of the risks of poor security governance.

Make data security guidelines simple and easy to understand, remembering that the average employee doesn't have the level of understanding of a CIO.

**Despite millions in infrastructure investment, organizations will continue to be affected by cyber incidents.**

This is due to a lack of training, not infrastructure, which allows a threat to become a security incident.

Ultimately, every employee needs to understand that securing their organization’s information systems starts and ends with them. If you fall victim to a phishing scam, hackers can easily access valuable data no matter the investment in information security systems and staff.

Sometimes it seems that the criminals have all the advantages, but that’s only the case when the organization is not vigilant and its employees are not committed to protecting it. Raise security awareness in your company, and talk openly about the issues and the organization’s expectations of good security practices. Acquire and install the best security technology you can afford. And then provide formal training to build the confidence and skills of security professionals and all users.
MINIMUM SECURITY FOR DESKTOP COMPUTING

PASSWORDS
Make a change every 30 days to your system sign-on, your online banking password, your email account password, and your password to any site that provides access to anything else. Those are the most important. You may not need to change the passwords for your fitness site and the place where you buy your shoes quite that often, but try to change all your passwords at least every 90 days.

Use strong passwords, and a different one for every site. If the system permits, use at least eight characters and compose them with uppercase and lowercase letters, numerals, and special characters (like #, &, @). You can get an application that will help you keep track of passwords, and some web browsers will do it for you, which means that you have no excuse for using the same password twice anymore.

One more thing about passwords: there is nowhere you can stick a Post-it® note that a thief can’t find, and if you stick a password to your monitor bezel, you pretty much deserve to be hacked.

TWO-FACTOR IDENTIFICATION
If a site offers you two-factor identification, take advantage of it. This is increasingly common and it’s easier to use than you might expect. During setup, you provide the site with a telephone number. Then, whenever you sign on, after you’ve provided your username and password, it calls you on the phone with a voice recording or sends a text message to give you a numeric code to complete the sign-on process.

MOBILE DEVICES
Use your mobile device’s protection. The iPhone®, for example, defaults to requiring a PIN or a fingerprint to in order to wake up (for anything but the camera). This means a thief is unable to use your iPhone for anything but taking pictures and can’t get to whatever sensitive information you have on the device or in the cloud.

SOFTWARE
Keep your OS software up to date. There are cybercriminals who dedicate their lives to finding vulnerabilities in the major operating systems. Once they do, the OS vendors are pretty good about patching the vulnerabilities and then automatically updating users’ systems. If you’re prompted to update your system (and if you trust that the prompt is not a phishing message), do it.

UNATTENDED COMPUTERS
If you need to be away from your desk for a few minutes, don’t leave the system open. Log out to protect your information from snooping. Some systems require a password when they wake from sleep. That means if you need to leave, you can just put the system to sleep. Don’t disable that feature. It goes without saying you should log off a public computer when you’re finished with it.

EMAIL
Even when you use a good spam filter, you should make your decision on whether to open an email message primarily on the FROM and TO fields and whether or not you expect the message. If you don’t know who it’s from, and it’s not addressed to you by name, it’s more likely to be spam, a virus, or a phishing attempt. Don’t be tempted to open a message just because a SUBJECT line sounds intriguing. Remember: every time you open a spam message, you encourage a spammer, making life more difficult for yourself and the rest of us.

TWO-FACTOR IDENTIFICATION
If a site offers you two-factor identification, take advantage of it. This is increasingly common and it’s easier to use than you might expect. During setup, you provide the site with a telephone number. Then, whenever you sign on, after you’ve provided your username and password, it calls you on the phone with a voice recording or sends a text message to give you a numeric code to complete the sign-on process.
Visit www.CFRcertified.com for more information or contact us at info@logicaloperations.com.

Headquarters - United States
3535 Winton Place
Rochester, NY USA 14623
U.S. and Canada: 1.800.456.4677
Other countries: +1.585.350.7000

International Sales Offices
China: +86-21-61763228
Latin America: +1.949.280.2312312
Europe & Africa: +011.44.208.397.8398
APAC: +65.9180.2305