Your cybersecurity CHECKLIST

The best practices you should consider implementing on a regular basis to protect your business from potential attackers

By Brent MacLean

Many of us are aware that IT security needs to be taken seriously and be an ongoing priority for all firms.

While no company or individual can be 100 per cent protected from cybersecurity threats, you can implement security best practices within a cybersecurity audit checklist, which can significantly reduce the risk of you becoming a victim of hackers or employee mishap.

KEEP YOUR OPERATING SYSTEMS UPDATED

Whether you run on Microsoft Windows or OS X, your operating system needs to be set for automatic updates. Turning off computers at night or rebooting promotes the installation of updates (as well as cleans out system clutter). System updates are especially important for server operating systems where all patches and updates need be reviewed and updated on a recurring schedule. Your employees need to be reminded to have their smartphones also set to update operating systems automatically.

ANTIVIRUS UPDATES

Firms need to ensure that anti-malware programs are set to check for updates frequently and scan the device(s) on a set schedule in an automated fashion along with any media that is inserted (USB thumb and external hard drives) into a workstation.

STRONG PASSWORD POLICY

IT policies should mandate complex passwords, meaning at least eight characters with a combination of upper and lower case letters, numbers and special characters. Network settings should require personnel to change their passwords four times per year and personnel should not be able to utilize any of the previous 10 passwords.

USE AUTOMATIC SCREEN LOCK

When a workstation or mobile device has been idle for a few minutes, it should be set to automatically lock the screen to keep prying eyes out of the system.

EQUIPMENT TRACKING

Know where your firm's data resides at all times. This includes, not only servers and workstations, but mobile devices, thumb drives, backup systems and cloud locations as well. Firms should strive to limit access to firm resources to only those staff who absolutely need it and have the proper security clearances.

SECURE DEVICES

Any device that contains firm and client data must be physically or digitally secured. On-premise file servers need to be in a locked room/cage and the office should have a security system. Mobile devices need to be locked when not in use and any data drives encrypted.

DISPOSE OF DATA/EQUIPMENT PROPERLY

All physical files and draft documents with personally identifiable information that is no longer needed should be secured and shredded to minimize the risk of dumpster divers accessing taxpayer IDs. Workstations and other mobile equipment used for processing client data should be thoroughly reformatted or the hard drive physically destroyed to minimize the risk of nefarious data recovery.

ENCRYPT BACKUP DATA

Firms should encrypt any backup media that leaves the office and also validate that the backup is complete and usable. Firms should regularly review backup logs for completion and restore files randomly to ensure they will work when they are needed.

MINIMIZE ADMINISTRATOR PRIVILEGES

Allowing workstations to run in administrator mode exposes the machine to more security threats. This can lead to the entire network being infected, so regular work should NOT be done on a computer in administrative mode, which IT should disable by default.

SECURE SEND

Firms should standardize tools that allow for the secure sending and receiving of client files. All personnel should be educated on using the firm's portal or encrypted email solution for any file containing confidential data.

CONNECT SECURELY

The IT team should train personnel how to connect securely to the firm's information resources either by utilizing a VPN (virtual private network) or other secure connection (look for the https in the web address bar). Staff should be reminded not to do any confidential work on public WiFi and only connect to WiFi for firm work if they are sure it is authentic (by verifying with the SSID/password with the client). Better yet, have them utilize a 4G LTE mobile hotspot or connect through that capability via their smartphone.

PROTECT MOBILE GEAR

While laptops have often been cited as the top mobile theft risk for many firms and other professional services, mandatory passwords and encryption should be extended to smartphones and tablets.

UPDATE IT POLICIES

Firms should review IT/computer usage policies and provide reminder training to employees at least annually for all new and updated policies. Beyond traditional computer and internet usage policies, firms should add wording on BYOD (Bring Your Own Device), remote access, privacy and encryption where appropriate.

EDUCATE EMPLOYEES

Security education is a vital aspect of managing any corporate entity. In addition to reviewing the firm's policies, employees should be educated on current cybersecurity attack methods such as phishing and pharming, and threats including ransomware and social engineering.

EMAIL AWARENESS TRAINING

Personnel need to be reminded to be skeptical of emails they did not expect and are out of character. Staff need to be reminded how to hover over an email link before clicking or to look at email properties to see if the sender's email address matches. They also need to be regularly reminded not to click on or open suspicious attachments. If there are any questions about a link in an email, it is better to go to the website directly by typing the address into a browser than to risk clicking on the link.

SCREEN POTENTIAL EMPLOYEES/ CONTRACTORS

Firms should do a thorough background check on all potential employees or contractors before allowing them access to firm resources. With today's internet connectivity and tiny USB storage devices, thousands of files can be covertly copied in minutes without anyone else realizing it and all a hacker needs is for the firm to grant access. Corporations need to be vigilant about employing all necessary security protocols when it pertains to the daily practices of the company's operations.

GREET OFFICE VISITORS

Employees should challenge anyone in the office they don't recognize and provide that person assistance if they have a pre-arranged meeting with a staff member. If the visitor appears suspicious, the employee should notify someone from management or administration immediately. So-called employees "shadowing," social engineering or stalking).

OUTSOURCE SECURITY

Hire expertise when implementing firewalls and security-related features such as remote access and wireless routers so that it is properly configured the first time. Chances are your internal IT people have not been exposed to optimum security training or have experience with setting up a new device. External resources can also be called upon to do penetration testing and risk assessments to identify and lock down any system vulnerabilities.

HAVE A BREACH RESPONSE PLAN

You should have a security incident response plan in place wherever there is concern that firm data has been compromised. This would be in a written format that would include educating personnel on how to document the events leading up to the breach discovery, notifying appropriate firm/external IT personnel of the breach so they can take necessary steps to stop it, and developing an internal and external communications plan.

CYBERSECURITY INSURANCE

Unfortunately, many firms can do all the right things in regards to information security and still fall victim to a hacker, so to protect against that possibility, they should consider cybersecurity insurance. The cost of this insurance has come down considerably in the last decade and firms should evaluate both first-party insurance to cover the firm's direct losses resulting from the breach (downtime, the re-creation of data, direct remediation costs) and third-party insurance to cover any damages to clients whose data may have been compromised.

DON'T HAVE A CYBERSECURITY AUDIT CHECKLIST YET?

Information security is everyone's responsibility and owners, stakeholders and department heads need to make a concerted effort to educate personnel and follow up on cybersecurity best practices to protect firm and client data.

And, while it's impossible to discuss every possible security scenario within the confines of a single IT article, it is this consultant's viewpoint that employing a strong Cyber Security Audit Checklist like this one, is a good way and a good start to reinforce your most valuable corporate assets and intellectual property.

Brent MacLean B.Sc.,M.Sc., is the CEO and senior security engineer at J.B. MacLean Consulting Inc. (jbmconsultinginc@rogers.com).