KNAV
PARTNERS BEYOND BOUNDARIES

Train your employees to avoid cyber crime

In an era of hyper-connectedness and a burgeoning global cybercrime industry, if you are in business, you cannot afford to just hope you will be lucky and avoid a successful attack. It's essential to establish policies and procedures to minimize risk to train employees on how to protect your business.

The basic kinds of criminal acts you need to guard against include:

- Theft of proprietary or sensitive business data that could be sold to competitors or other hackers;
- Installation of `ransomware' that locks you out of your own data until you pay the cybercriminals' demands;
- Malicious damage to your system, such as crashing your website to prevent customers from accessing it; &
- Theft of employees' personal information to eventually steal from them.

Internal threats

Building a defensive strategy starts with recognizing that, even with the best technical external barriers in place, you can fall victim to an employee who goes rogue, or even joins your organization specifically with cyber crime in mind.

While unlikely, it's essential for your hiring managers to be mindful of these risks when reviewing employment applications, particularly those for positions that involve open access to sensitive company data. It's just another checklist item when reviewing applicants with unusual employment histories. Checking references and conducting background checks is also a good idea.

In the same way, it's generally advisable to include a statement in your employee handbook informing employees that their communications are stored in a backup system and that you will reserve the right to monitor and examine their company computers and emails *(sent and received)* on your system.

When such monitoring systems are in place, prudence or suspicious activity will dictate when they should be ramped up.

Department of Homeland *('DHS')* security tips

It can also be useful to establish a policy encouraging employees to report any suspicious computer-based activities they observe. Of course, you don't want to foster employee paranoia or promote the spread of baseless accusations. But deploying more eyes and ears can serve both to forestall cyber bad behaviour and detect it if it occurs.

The largest threat is not that employees may intentionally commit cybercrime, but that they might inadvertently open the door to external cybercriminals. That's why DHS considers cybercrime serious enough to offer these eight tips for employers to pass along to their employees:

- Read and abide by the company's Internet use policy;
- Make passwords complex; use a combination of numbers, symbols, and letters *(uppercase and lowercase);*
- Change passwords regularly *(every 45-90 days)*;
- Guard usernames, passwords, or other computer or website codes, even among co-workers;
- Exercise caution when opening emails from unknown senders, and don't open attachments or links from unverified sources;
- Do not install or connect any personal software or hardware to the organization's network or hardware without permission;
- Make electronic and physical backups or copies of critical work; &
- Report all suspicious or unusual computer problems to IT personnel.

Employees that follow these steps faithfully can serve as an additional layer of protection against cyber attacks.

For those people who are charged with the responsibility to maintain a secure system, the DHS offers the following advice:

- Implement a layered defense strategy that includes technical, organizational and operational controls;
- Update the existing anti-virus software often;
- Follow organizational guidelines and security regulations;
- Regularly download vendor security patches for all software;
- Change the manufacturer's default passwords on all software;
- Encrypt data and use two-factor authentication where possible;
- If a wireless network is used, make sure that it's secure; &
- Monitor, log and analyze successful and attempted intrusions to the company's systems and networks.

Cyber crime insurance

What else can be done? It's often a good idea for businesses to protect their computer systems further by buying cyber crime insurance. Alone, this won't prevent victimization, but it can offset some of the financial damage in case of a successful attack.

In addition, most insurers perform a rigorous risk assessment before issuing a policy and setting premiums. The results of such an assessment can be quite eye-opening for business owners.

If you decide against buying insurance, it might be useful to have a consultant conduct a cyber crime exposure risk assessment anyway. The growth, ubiquity and high cost of cybercrime has spawned a large industry of cyber security consulting firms. And, unless your company already has a robust IT staff with expertise in cyber-risk mitigation, you'll likely save time and money engaging in a third-party vendor.

Courtesy: EGP PLCC