CYBERSECURITY

Why technology is not enough to fend off a cyber attack

Authors
Chami Akmeemana and Guy Pearce

Fending off cyber attacks needs more than the best anti-virus technology -- it also demands a shift in culture.

Our research shows that while smart technology may be necessary to keep malware, viruses and other forms of electronic intrusion at bay, it is not sufficient. Rather, the weakest link often turns out to be people who are either careless or not properly trained in cyber-security processes.

For example, ransomware (which encrypts files and then demands payment before restoring the data), is usually introduced into an organization's computer system when an unsuspecting employee clicks on a link embedded in an email that is thought to be legitimate. Earlier this year, the US Federal Financial Institutions Examination Council (FFIEC) warned banks about a continued sharp rise in cyber-attacks using this type of malware.

User error, loss of equipment, insider sabotage, spam and phishing….these are all examples of how even the best software cannot protect a company or government department if its employees fail to stick to the rules. The role of human beings in cyber risk is so significant that PwC, a leading consultancy, once cautioned that "employees are the most-cited culprits of incidents."

It is true that technology can mitigate the risk of human error through the use of warning signals, passwords, and other security devices. Even so, any chief executive who assigns total responsibility for managing cyber security to the technology or IT department is taking a big risk.

So how can we address the risk posed by careless, badly-trained or malevolent people?

First and foremost, develop and instill a strong risk culture in your organization.

The Financial Stability Board (FSB), a body that monitors and makes recommendations about the global financial system, says that a shared understanding of an organization's risk culture is "crucial" so that everyone knows what behaviour is expected of them.

> Deloitte, another big consultancy, believes that "cyber-security leaders . . . want to instill a 'cyber-security culture' in their organizations."

In other words, developing and integrating an appropriate risk culture should be an important corporate governance goal, not just for senior executives but also the board of directors. It's vital to set the tone right at the top.

According to the FSB, a strong risk culture begins with a senior leadership team that is transparent and open to criticism, that has documented all risk management responsibilities, and that encourages desired behaviour. The culture they instill then guides the behaviour of colleagues throughout the organization so that it becomes second nature for everyone to act in ways that help mitigate cyber-risk.

At the GRI, we believe this requires the establishment of a robust governance structure that sits atop the many silos of a large organization. Among other things, this structure should include a cyber security orientation program for new hires (including board members), an internal control framework, an annual testing and certification process for employees, and an incident reporting system.

It should also involve constant attention to the policies, procedures, standards and guidelines demanded by an effective cyber-risk strategy, in other words, obeying the rules. But it also means more than that. Senior executives must set an example through their own behaviour. Key cyber-security messages must be constantly repeated. And there must be a way of measuring implementation of the rules so that weak spots can be quickly identified.

The human resources department can—and should—play a key role.

HR should partner with senior management and the board to identify the drivers of people risk, and then draw up a plan to correct shortcomings. That plan should be cemented into the corporate culture through a company-wide transformation program. Some organizations see this as a training activity. However, a coordinated response to one of the biggest risks that a business faces needs to have a higher priority than, say, a one or two-hour training course.

Developing a risk culture can be costly and time-consuming. But the effort is sure to be worthwhile. An effective risk culture can boost productivity, and thus have a positive impact on earnings, and on the value of the organization. It's not hard to imagine that a tightly integrated risk management strategy could become self-funding as the potential benefits start to match the costs.

As the new cyber risk culture takes hold, every person in the organization, no matter what their job, becomes a line of defence, not only against cyber attack but against business risk in general. That benefit alone is a commanding reason to develop and integrate a risk culture into your organization.

The bottom line is that cyber risk management is much more than an IT issue. Senior management and the board have a duty to inculcate risk culture into the organization so that everyone works as a team to fend off cyber and other risks.

Technology is, of course, a critical enabler of that strategy, but it is not a strategy on its own. Any company that believes it can put its faith in technology alone should steel itself for the worst.

As published in the American Banker July 2016

COMMENTARY

"The connection between risk culture and cyber security is very important for any organization to understand and to manage. Risk culture is now not just about stopping rogue traders but very much about how an organization's employees think about risk in their day to day actions. A strong risk culture is an increasingly important defence against cyber attacks, particularly as the use of social media increases for business uses".

Mark Hughes
Global Chief Risk Officer, RBC

"Creating a secure environment for business and consumers is about more than installing firewalls. Cyber security needs to be a partnership between

public institutions, businesses, and consumers. The first line of defence is a well-established, strong risk culture, which involves not only layers of security and constant vigilance, but also cutting-edge knowledge, expertise, co-operation, and awareness to safeguard the privacy and integrity of information and systems".

Laura Dottori-Attanasio
Senior Executive Vice-President & Chief Risk Officer, CIBC

"Cyber risk is rapidly evolving and expectations with respect to how companies plan and execute their risk mitigation activities will continue to escalate. It is dangerous to think that this is just an 'IT' issue, rather this involves a co-ordinated multi-discipline approach across an organization. At a basic level it can be as simple as how individuals react to incoming 'phishing' emails; the reality is events will happen, which in my view makes a robust response plan one of the most important aspects of Cyber Security."

Rodney Hill
Chief Risk Officer, OMERS

"Within the past few years the number of true cyber-related crimes has dramatically increased. These have included system hacks, DDoS attacks, crypto-extortions, and large scale data breaches. Additionally, criminals are increasingly turning to the internet to facilitate more traditional forms of crime, such as fraud, extortion, money laundering and the distribution of contraband. Consequently, The Ontario Provincial Police has developed a strategy to position the organization to manage risks, reduce threats and minimize harm caused by crime involving digital technologies. The primary focus of the strategy is to increase the OPP's enterprise-wide capacity to deal with cyber and cyber facilitated crime. The strategy's centre-piece is a tiered response model makes the response to cybercrime a shared responsibility by every member of the organization. The foundation of the tiered response model is good "Cyber-Hygiene." In addition to training on cyber security all 9,000 members of the OPP will receive the same simple message – good cyber security and the organization's ability to respond to cybercrime is the responsibility all members and needs to be a grassroots movement".

Paul Beesley
Superintendent, Ontario Provincial Police
Responsible for the development and implementation of the OPP's Cyber Strategy

"Cybersecurity can no longer be viewed as an IT issue. Unfortunately, far too many organizations still believe this and so it doesn't get the executive leadership attention it requires. Cybersecurity is an enterprise issue. This means it must be a priority for the board, for the CEO and the entire C-suite, and then across all management and deep into the organization. If an organization gets hit by a significant cybercrime the implications are far greater than most anticipate. There will be economic losses--that could include ransoms; recovering from the attack; and damage to brand. Even a modest attack can cost an organization in the millions of dollars. It's time for all of leadership to step up to the challenge".

Dr. Jonathan Reichental
Chief Information Officer, City of Palo Alto

"Through the fast expansion of online usage together with various method of cybercrime, cyber security is not an IT issue any more. Asia is not an exception on this matter but not very well aware yet. The connection between risk culture and cyber security should be executed through the whole company from the management to each individual staffs since the loss and damage from this cybercrime is far above from our imagination. It's the time to head up by all management lines and relevant department such as HR, Compliance not only IT."

Younjeong Lim
Chief Risk Officer, PingAn Puhui, China

"In the new world of Cyber risk, using the traditional tools, techniques and approaches together with an over-reliance on technical solutions will be a losing battle. Organisations need to bolster their capabilities and to think differently – they need to ensure they boost their Cyber teams with psychologists, futurologists and those that can think creatively. Further, organisations need to be able to deal with a wide variety of threats faster than ever before. Implementing the concept of Agile Cyber improvement linking to people, processes as well as technology is fundamental , and should be a core part of any security strategy".

Paul Hanley
Partner KPMG, National Leader
Cyber Security Services

"If the strategic leadership pays appropriate attention to the cyber security at the organizational level, it reduces the attention that should be paid by the employees at the operational level. For example, nowadays it is impossible to identify at the user level whether or not a link in a received e-mail is malicious or not. One additional dot or a changed letter in the link is sufficient to make it malicious. Compare: globalriskinstitute.org and globalriskinstitute.org These links seem identical. In the first case the link is correct. In the second case the first small letter l is changed with the capital letter i (I). The user doesn't notice the difference because the small letter l and the capital letter i look the same. But this change is sufficient to direct a user to a malicious website and conduct an attack against the organization.

There are certain aspects of cyber security, which could not be solved at the user level. User-level training and awareness is never sufficient in order to deal with this kind of challenges. It means that the strategic leadership should be aware of modern cyber risks and implement technologies and procedures, which solve the cyber security challenges at the strategic level and reduces the cyber security responsibilities at the user-level. This brings us back to the question of a culture of security. If the security culture is strong in the organization and it is led by the senior leadership than most of the cyber security problems are solved at the strategic level and employees can concentrate on their daily tasks".

Raul Rikk
Head of Cyber Security,
e-Governance Academy Foundation, Estonia

About the Authors

Chami Akmeemana is Managing Director of Global Markets at the Global Risk Institute.

Guy Pearce serves on the Board of the International Institute of Business Analysis and is a consultant specializing in strategy, risk, data and technology.