The GlobalEthicist

Cyber-insecurity – the chief risk and reputation officer's role

It doesn't matter how big or small your organisation: these days you are under threat from cyber-attack, warns Andrea Bonime-Blanc

Everyone has heard about cyber-security, cyber-hacking, cyber-terrorism, cyber-fear, cyber-espionage, cyber-war – especially in the wake of the recent US National Security Agency whistle-blower scandal, which continues to unfold and make the headlines.

Let's assume you are your company's chief risk and reputation officer (CRRO) or someone who manages ethical, reputational or other operational risks within your organisation.

You read about the global banks that are being cyber-attacked daily by obscure third parties seeking personal bank account information; about the infrastructure companies whose key assets may be at risk, leading to possible crises involving the shutdown of an urban, regional or even national electrical grid, for example; or about international economic espionage using cyber-technology to infiltrate company computers to target and steal intellectual property and other valuable secrets such as M&A plans, business strategies, product formulas, trade secrets and patents.

We're all hacked

Whether politically driven (government-sponsored spying), economically driven (criminal rings) or anarchy driven ("hacktivists"), the cyber-era has arrived and no one, including governments and their national security agencies, seems fully prepared to deal with the attacks, infiltrations, disruptions and pure chaos. It is the dawn of the era of cyber-insecurity.

What are you, a CRRO, a risk manager, a concerned businessperson or board member, to do in the face of this overwhelming and complicated set of cyber-issues? What do these issues mean to your company? What are you supposed to do – as a professional and as a person? What are the vulnerabilities of your work environment? Have you become a target? Have you been infiltrated yet? Is anyone in your organisation acting proactively and fully equipped to deal with this issue? Do you have an overarching strategy or governance mechanism to meet this new and constantly evolving challenge? What is your board's perspective on this, if any?

These questions don't just apply to highly visible and vulnerable infrastructure and banking institutions. They apply to just about any type of organisation, located anywhere in the world, regardless of size, scope, focus, mission or personnel. It applies to for-profit, non-profit, academic and governmental entities. US FBI director Robert Mueller recently said: "There are two kinds of companies – those that know they have been hacked and those that don't know but have been."

Technological disruption and cyber-mayhem gets complicated further by the multiple and ever-changing sources and types of cyber-threat. There's the brilliant teenage hacker sitting in his basement infiltrating high value governmental targets mainly for the "fun" of it; there's the highly organised criminal underworld rings that steal identities; and then there's governmentally sponsored industrial espionage and national security cyber-activity up to and including cyber-war.

Types of cyber-threat can be indiscriminate or highly targeted and can range from moderately innocuous to decidedly dangerous. There is an ever increasing spectrum of possibilities, from viruses to malware to password and account infiltration.

In the face of what will continue to be a very

Technological disruption gets complicated by the multiple sources and types of cyber-threat

COLUMNIST: ANDREA BONIME-BLANC

confusing, constantly changing and increasingly dangerous cyber-environment, it is still possible for an organisation and its CRRO (or equivalent executive) to construct a framework and a plan to deal with these issues proactively.

First, you need to know the extent of your cyber-problem – and remember everyone has a cyber-problem. There is no size cut-off, no type of entity that isn't vulnerable, no cause too small. While certain industries are favoured targets (financial, infrastructure, defence, technology), everyone is cyber-vulnerable.

Cyber-vulnerability comes in many forms, ranging from the innocuous but still pesky infected email attachment that turns into an annoying virus on your computer or system to a full frontal advanced persistent threat (APT), which can take many forms and many routes. The former is something your information security/technology team can usually fix by having the right anti-virus software and updates installed. The latter is much more complicated, requiring a full set of defensive and proactive solutions.

You need to know who's in charge – or not. Who manages your company's information security needs, not just information technology requirements? What is their background and expertise? What do they know and what don't they know? Do they know what they don't know? Do your internal experts – in IT, information security (infosec), audit or risk management – have the right kind of expertise for your type of organisation?

Whether you have the right internal experts or need to bring those experts in from the outside, you should run a baseline cyber-vulnerability risk assessment on your system so that you have an understanding of your gaps.

As part of your technical vulnerabilities risk assessment, you also need to gain a full understanding of your subject matter or target vulnerabilities. In other words, brainstorm what the specific targets of opportunity are within your organisation that may be of value or interest to hackers, criminals and spies. For example:

- privacy-protected information: names, addresses, accounts, identification;
- HR databases;
- health information;
- business strategy and financial information;
- technology and other intellectual property;
- network and servers; and
- infrastructure assets.

Critical steps

Enlist management. Find someone within your organisation at the highest level who will listen, understand the threat, know what they don't know, be influential in enlisting other executives and help champion this issue until it is properly addressed.

Create an internal awareness programme through policies, training and communication. If people don't understand how the threat penetrates the system at the individual level, your defences will be as good as your weakest link within your company – the uninformed, careless employee or worse, third party contractor.

Have a crisis management plan that incorporates cyber-vigilance. This is critical and non-negotiable for any organisation that cares about its stakeholders and about business continuity. From a crisis management standpoint, a cyber-problem can come in three sizes – and you should be prepared to deal with all three:

- **Limited:** localised, limited concern. For example, a virus has infected a limited number of computers in one location.
- **Critical:** larger scale, more widespread, critical concern. For example, an important office is shut down by malware which threatens to infect other parts of the organisation globally.
- **Existential:** a widespread, possibly life-threatening disaster takes place, with a threat to or loss of life, or asset destruction.

Form an IT/infosec governance committee. Consider the formation of a high level global committee that serves as a global governance body helping to assess overall policy on cyber-threats and insecurities on an ongoing basis for the organisation. Members should include legal, audit, IT, senior management (up to and including CEO or COO) and of course the CRRO or equivalent. The agenda of this committee should track the cyber-security gap risk assessment and tie overall policy back to the business purpose and strategy of the organisation.

Finally, get your board on side and keep them posted quarterly or even more often if serious events occur. Understand what your senior executives and board understand or don't understand about this issue. Get a risk management framework in place, if you don't already have one, to manage this issue and keep executives and directors informed, real time.

In today's world, it is a duty of every organisation to gauge its cyber-profile and vulnerabilities, no matter how small and unrelated it may think it is to the big bad world of cyber-crime. Cyber-vigilance is the new name of the game and the very least an organisation owes its stakeholders is to understand what its possible exposure is and to guard against the exploitation by outsiders.

The cyber-world presents a complicated, multi-faceted, ever-changing set of threats and risks. The CRRO is in a unique position to help address these complex issues. While not necessarily the infosec expert, the CRRO is the expert risk and reputation executive, someone who sits on the leadership team and reports regularly to the board. The CRRO can bring it all together, package the issues in digestible and understandable portions, present the risks in a compelling, business-savvy way to his or her colleagues and the board and help drive and lead the ongoing solutions. ■

Top 10 must-do actions

1. Engage the right **internal functional expertise**.
2. Engage the right **external** expertise.
3. Engage the **chief executive** and the right **senior people** in your organisation.
4. Conduct an infosec **baseline risk assessment** including third party supply chain cyber-vigilance.
5. Incorporate cyber-vigilance into your **crisis management** and **business continuity** planning.
6. Communicate, communicate, communicate, and train your **employees** and **consultants** on cyber-vigilance.
7. Empower the **infosec function** and include them in your governance structure with sufficient **budget** and **tools** to be informed and carry out defensive and proactive work.
8. Know your **legal obligations** within your headquarters' jurisdiction and other operational locations, including disclosure duties if you are publicly listed.
9. Consider creating a high level IT/infosec **governance committee** headed by a high level executive (including the CEO).
10. **Engage your board** regularly and periodically.

Dr Andrea Bonime-Blanc is chief executive of GEC Risk Advisory, a governance, risk, ethics, compliance and corporate responsibility management consultancy. She is chair emeritus of the Ethics and Compliance Officer Association, a member of Ethical Corporation's editorial advisory board, and a life member of the Council on Foreign Relations. @GlobalEthicist