Advisory

Computer network

Advisory Alert: Think like a cybercriminal to combat threats

The hospital's boardroom is packed. Leadership, department heads, administrative heads and board members are meeting, and a sense of gloom pervades the room. It just may be the end of their world as they know it. A high-profile celebrity patient is dying upstairs. At first it was seen as a medical mistake, but now something more sinister appears to have happened. The news is spreading through social media that the patient is close to death because of a hack into the hospital's systems. Protesters are already gathering out front, asking for a temporary hospital shutdown.

Ojel Rodriguez
Partner Head of Advisory
Kevane Grant Thornton
T (1) 787 754 1915
E ojel.rodriguez@pr.gt.com

Visit our website
www.grantthornton.pr

Introduction

The CEO demands to know how it happened, especially after a recent multimillion dollar investment in improving the hospital's cybersecurity program. The technology team started explaining what they thought happened, describing how they implemented a perimeter security system designed to prevent hackers from gaining access to patient credit card data and health records. In this case, however, the hackers didn't go for any of that — they went straight to the celebrity patient's registration and real-time blood test data and changed his blood group, which resulted in an incorrect blood transfusion. There was a ransom call, but the hospital was too slow to react. The surgery started and the doctors used the wrong blood type, to disastrous effect. The patient is left irreversibly damaged and is expected to die within 24 hours.

The CEO addresses the room with fire in her eyes and says: "How could this have happened? Our business is patient **care** and not patient **data**. We've approached this the wrong way. Fix it!"

Fortunately, this was a cyberwar gaming exercise that Grant Thornton LLP was engaged to perform by one of our hospital clients.

Conventional thinking on cybersecurity is that it is past its expiration date. Companies spend big money to head off cyber-threats, with mixed success. Meanwhile, business leaders routinely acknowledge that attacks against their organization aren't a matter of if, but when. Their nervousness is driven by everyday scenarios of cyberattacks turning into business crises. What's a forward-looking enterprise to do?

The journey from reactive to proactive cybersecurity starts by understanding what is important for the business to grow and thrive.

Reaching a higher state — cybersecurity preparedness 2.0 — forces organizations to acknowledge that they live in an evolving environment. Companies must accept that digital innovation is at the heart of business growth. They must recognize that data is an outcome of that innovation. And they must admit that data can also be a liability. Leaders have to be willing to step into the shoes of cybercriminals, understand the potential motivations and threats these bad actors pose and ultimately come up with proactive strategies to protect their organization's interests.

The journey from reactive to proactive cybersecurity starts by understanding what is important for the business to grow and thrive. The weakest link might be a technology issue plaguing a retail brand. It could be a strategy issue in a life sciences organization. Or it could be a process issue in a financial services enterprise. Regardless of the industry, fostering an understanding of what is truly important for the business is foundational to establishing a sound security strategy.

Treating cyber-risk as separate from other business risks renders it overly technical and mysterious. A more holistic approach to cyber-risk allows companies to place cyber-risks in their proper strategic context and show how management's acceptance of specific cyber-risks will assist — or fail to assist — in creating value. Businesses that fail to enact a strategic approach, and don't include all senior managers in defining and meshing their roles in confronting risk, will continue to be stuck at cybersecurity 1.0.

There are a few obvious hallmarks of companies that are relatively immature on the data-security spectrum:

Letting fear set the agenda

Cyber-breaches can result in costly losses and embarrassing headlines, but fear of breaches can focus management exclusively on point-specific, IT-centric solutions that are regularly leapfrogged by cybercriminals.

Undervaluing digital assets

Companies often assign values to physical assets, but many fail to grasp the true value of all their data, intellectual property and intangible assets such as brand reputation, executive reputation and customer trust. What's more, companies frequently fail to assess the full costs of operational, financial and legal risks that stolen data, compromised transactions and corrupted systems can generate.

Doing an unsatisfactory job defining cyber incidents

These include not only external attacks, but also internal breaches, natural disasters and other events that affect systems and data.

Adopting cyber capabilities without enough strategic contexts

Companies often adopt new technologies — such as mobile devices, social media, cloud computing and artificial intelligence — or form new external partnerships, without considering the full array of risks to their business strategies and changes in their risk appetite that these new ventures may introduce.

The emerging universe of risks will run the gamut — some will be technology issues, but others will be business issues or process issues or people issues. But you'll never know unless everyone is linked to the same effort. Achieving this kind of collaborative approach begins when everyone in a leadership position recognizes the stakes. Getting there requires a few logical steps:

1. **Own the predicament.** Cybersecurity is a top concern of global leaders, as seen in the World Economic Forum's *Global Risks Report 2017*. The issue topped the list of most likely risks in North America. For context, consider that more than five million new devices are activated every day. Analysts predict the number of internet of things devices will soar from more than six billion today, to more than 20 billion by 2020. Connectivity equals risk, and therefore everyone is responsible for cybercrime prevention.[1]

2. **Map business processes, stakeholders and data systems.** Organizations focused on cyber-risk need to adopt the kind of seamless, crash-free and bug-free approach that we see on popular mobile apps — a full-stack view of your assets, consisting of full mapping of business processes, the potential users and related technologies. You need to weigh your cyber-risk by conducting risk assessment of each asset (stack view). Only then is it possible to identify potential risks, consider those risks against risk appetite, and implement controls accordingly. Where risk is elevated, controls need to be higher.

3. **Align, integrate and measure.** It is vital to bring together operational and financial leaders with risk leaders, and align and integrate their goals, objectives, compliance demands, and stakeholder expectations. This will require operational processes to be meshed with cyber controls — with a special focus on where the business is most sensitive. And all this must be overlaid with a system of measurement and metrics, so that leaders always can assess the threat outlook, have options to dial up controls and further enact a digital strategy.

[1] "6.4 billion connected 'things' will be in use in 2016," Gartner, Nov. 10, 2015.

Source: https://www.grantthornton.com/library/whitepapers/advisory/2017/think-cybercriminal-combat-threats.aspx

Conclusion

The key to managing threats isn't necessarily greater investment or even manpower. Instead, it takes the imagination of a criminal — seeing your own enterprise as they would see it. Wherever you are most sensitive is the most likely target of future cyber-threats. What is most valuable to you is also most valuable to someone who wants to hurt you.

Kevane Grant Thornton
An instinct for growth™

DISCLAIMER: This update and its content do not constitute advice. Clients should not act solely on the basis of the material contained in this publication. It is intended for information purposes only and should not be regarded as specific advice. In addition, advice from proper consultant should be obtained prior to taking action on any issue dealt with this update.

Kevane Grant Thornton LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please visit www.grantthornton.pr for further details.

grantthornton.pr