WIPRO CONSULTING SERVICES

WIPRO
Applying Thought

Cyber Warfare, Governance, and the Art of War

www.wipro.com/consulting

Cyber Warfare, Governance, and the Art of War

By Manohar Ganshani

It was a catastrophic Christmas for retailer Target, which had to admit that its customer data was hacked, resulting in the theft of close to 40 million credit and debit card records and some 70 million other records holding customer information. That was followed by news of a breach of luxury retailer Neiman Marcus' data, which caused more than a million credit and debit cards to be compromised.

Last year, giant corporations including the New York Times, Wall Street Journal, Apple, Facebook, LinkedIn, and Twitter reported security breaches, while hacking has also hit the governments of South Korea and China. Given this track record, it's clear that no one is immune, and every organization must be on the offensive to ward off attacks. In a very real sense, these are acts of war—cyber war.

When it comes to war, it's not uncommon to hear people quote the ancient Chinese military general, strategist, and philosopher Sun Tzu, whose tenets apply here. As he wrote:

"If you know the enemy and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, for every victory gained you will also suffer a defeat; if you do not know your enemies nor yourself, you will succumb in every single battle."

Add to that, "Speed is the essence of war."

I look to these among his 144 famous quotes because they reflect the key aspects of good governance in the age of cyber warfare. Knowing your enemy and yourself means you understand their vulnerabilities and strengths just as well as you understand your own. It means you have threat intelligence; and with situational intelligence you can achieve speed.

Technology is the weapon of choice in cyber warfare, and between the two sides it's become the equivalent of an arms race. But despite the fact that most organizations have the best technologies in place, they're either still under attack or they fear the potential for an attack. All of which suggests that it's not so much the technology that needs reassessing, it's the governance around people and processes.

A Solid Governance Strategy

It would be a reach—and, indeed hubris—for any organization to say it's absolutely certain of its ability to fend off cyber attacks.

As technology evolves, hackers look for software vulnerabilities. So superior cyber security means having a relentless, high-stakes effort to identify and predict those vulnerabilities and erect defenses against them.

But the best cyber security defense goes beyond technology considerations. It also means superior governance. In its truest sense, governance has to do with ensuring effective decision-making, investing in the most strategic places, and establishing an effective response mechanism.

Let's start with the basics—your people. If people are your organization's greatest asset, they're also your greatest vulnerability. So you must institutionalize the right culture through systematic detection and reporting of security incidents. To be effective, you must have skilled people to champion your user awareness. You must know who is doing what, where your data is, and how secure it is.

> *In its truest sense, governance has to do with ensuring effective decision-making, investing in the most strategic places, and establishing an effective response mechanism.*

That's at the most fundamental level. In order to get a more crystallized picture, however, a comprehensive audit will help you benchmark where your organization stands if a security breach, incident, or hacking attack takes place—and how quickly and effective your response is. There are also lessons to be learned from breaches that have occurred at other businesses. This contextual and situational intelligence tells you where you should prioritize your focus and invest effectively.

A solid governance strategy focuses on five basics:

- **Sharing threat intelligence**. You need real-time, systematized, and automated sharing of threat intelligence between the public and private sectors or across heterogeneous groups of international enterprises. This can be achieved by building a trust model among your peer groups or heterogeneous groups.

- **Conducting an outside-in scan to learn the value of the business at risk.** Bring in an external expert to test your governance capabilities around four basic items: internal ecosystem networks, social networks, locational data, and dark Internet (conventionally unreachable network hosts on the Internet) linked to critical processes and assets. It's about diagnosing, benchmarking, and letting you know where you stand.

- **Securing your supply chain**. Evaluate emerging threats throughout your supply chain and assess your risks. For example, a bank experiencing a cyber attack may have connections or interdependence with other banks or third parties that could then be at risk.

- **Embracing speed.** Put in place a standard risk-based process for decision-making. You need to establish who should make what decision and in what timeframe. Measure the effectiveness of your procedures for handling incidents and your team's ability to take action on them. That's the key parameter for immediate response capability.

- **Developing effective response expertise**. This is the most important piece. Create a task force of highly skilled cyber specialists and security and forensics experts who understand networks, systems, and incident management. Evaluate your organization's preparedness to respond and resolve threats originating from the unknown. It's unconventional, but you might even consider hiring hackers to simulate full-blown attacks to test your readiness.

Creating Your Strategic Governance Plan

Accountability in an organization can no longer rest solely with the chief security officer (CSO). It must be with the CEO and the board of directors. One way to create awareness at the beginning of a governance program is to develop a Responsibility Assignment (RACI) Matrix, which clarifies roles and responsibilities for your cyber risk program. The CSO can champion the cyber security program with the help of peer groups within Audit, Finance, IT, and Administration to achieve necessary and timely buy-in from the start.

This will lead to the creation of your "cyber cell," basically a high-power committee that can be comprised of the functional heads of IT, Security, Audit, Legal and Compliance, Finance, and HR—all chaired by the CEO. The cyber cell's role is to shape your strategic governance plan and, when necessary, make on-the-spot decisions, including funding event response.

Once you have the right people in place and have created a cyber cell with fixed roles and responsibilities—all based on your outside-in scan—you'll create a strategic governance plan essentially based on three components:

- Developing basic elements like security policies and threat and vulnerabilities profile—regularly updated and referenced

- Identifying the right set of partners, aligned with your strategy, to work with you on an ongoing basis as well as during an event. They should go beyond the obvious to share with you trends, implications, possibilities, and solutions.

- Defining a response, incident, and communication management plan

One approach to launching your governance plan is to do a pilot project. Conduct a quick internal assessment on how you think you score on your strategy and your plan. As a next step and to validate your own assessment, engage an expert firm to test your assessment and benchmark against standards and guidelines established by international government defense agencies. Choose a firm that knows what regulators want and has domain knowledge of your industry. Then you can begin to develop your governance strategy around the five basics described above.

A Foundation for Security

Cyber risk is a moving threat agent. As cyber risks increase, there's no doubt that your technology must be kept up to date. But it's the governance around your technologies and your people and processes that will help reduce the threat of attack and mitigate the fallout if you're struck.

You are a soldier in a cyber warfare army. Know yourself, and know your enemy. Establish a sound plan, and be quick in response to any attack. Your customers, your investors, and your organization are counting on it.

Manohar Ganshani is Partner and Global Practice Head of the Governance Risk & Compliance Practice of Wipro Consulting Services. He is based in London and may be reached at manohar.ganshani@wipro.com.

About Wipro Consulting Services

Wipro Consulting Services helps companies solve today's business issues while thinking ahead to future challenges and opportunities. As a business unit of Wipro, one of the world's leading providers of integrated consulting, technology, and outsourcing solutions, we bring value to our clients through end-to-end business transformation – think, build and operate. Our model for the *21st Century Virtual Corporation*℠ includes implementing lean process transformation, exploiting new technology, optimizing human capital and physical assets, and structuring next generation partnering agreements that create value and win/win business outcomes for our clients. For information visit **www.wipro.com/consulting** or email **wcs.info@wipro.com**.

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology" - helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation, and an organization wide commitment to sustainability, Wipro has a workforce of 140,000 serving clients across 61 countries. For more information, please visit www.wipro.com.

WIPRO
Applying Thought

DO BUSINESS BETTER

WWW.WIPRO.COM NYSE:WIT | OVER 140,000 EMPLOYEES | 61 COUNTRIES | CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL: +91 (80) 2844 0011, FAX: +91 (80) 2844 0256 email: info@wipro.com

North America South America Canada United Kingdom Germany France Switzerland Poland Austria Sweden Finland Benelux Portugal Romania Japan Philippines Singapore Malaysia Australia