February 2015

Knowledge@Wharton – Wipro

CIO Series

Embedding a 'Culture of Security' Is the Best Defense

Knowledge@Wharton – Wipro

CIO Series

Embedding a 'Culture of Security' Is the Best Defense

Increased connectivity and data use have greatly heightened the risk of a major security breach. But on top of the requisite technological protections, one of the best security defenses organizations can have is a "culture of security," says Robert Coles, chief information security officer at GlaxoSmithKline. He and Sigal Barsade, a Wharton management professor, and Sheetal Mehta, global head of enterprise security solutions at Wipro Technologies, delve into this idea in this CIO Series article, produced by Knowledge@Wharton and sponsored by Wipro.

Robert Coles, chief information security officer at pharmaceutical and health care company GlaxoSmithKline (GSK), is in the midst of putting together a team that will be embedded in the firm's business divisions. The team will work closely with strategists and planners who come up with new ideas and innovations to ensure that security is integrated in the early stages of any change. Coles, who has been with GSK for just over a year, says: "You can secure anything if you think about it while developing it. Unless it is embedded early on, it becomes very difficult and costly, and it's almost impossible to get the required level of security."

High profile security breaches at companies like Target and Home Depot have underlined the damage that can arise from a single security breach. And while those two examples came from the world of retail, most companies house sensitive information that could be valuable to hackers.

Meantime, the risks of a breach mount daily — a result of increased connectivity and rising data use as the world of big data morphs through organizations. "Historically we had one pipe that connected our network to other organizations and we could protect that pipe easily," says Coles. "Now, everything is connected to everything through the Internet, so the surface of attack is much more. Also, a lot more information is used to manage any business. Therefore, the size of the prize for the attacker is much greater."

Sheetal Mehta, global head of enterprise security solutions at Wipro Technologies, adds that the present business environment demands that organizations work collaboratively. Users are also more empowered. "This makes the organizations susceptible to new risks and increased attacks."

> *"Security must be top of mind and needs to be a day-to-day function of each individual."*
>
> — **Sheetal Mehta**

Typically, there are two levers for ensuring information security. One is highly technology centric and comprises processes, controls, rules and regulations. The other is the culture of the organization — its values, beliefs, principles, behaviors and managerial practices. Sigal Barsade, a Wharton professor of management, believes that organizational culture is a critical lever.

"Culture is the shared cognizance. Simply put, it is what employees know they are supposed to do when the boss is not looking. When it relates to issues like information security or compliance, the most effective means for a company to protect itself is for its employees to understand that it is a critical value for the organization — that regardless of whether someone is looking over them or if procedures are in place, they should be following the security measures because that is simply the way the organization works." Since culture is a socially accepted norm, in some way or the other everyone polices each other, she adds.

Behavior Makes Technology Effective

It is very easy to deploy technology, Mehta notes. But employee behavior and concrete action make technology effective. For instance, technology allows for resetting passwords periodically, but it takes behavioral change to ensure that the right kinds of passwords get used. Or, if someone loses their entry card, they must report it immediately to the central security group. "Security must be top of mind and needs to be a day-to-day function of each individual," says Mehta.

Adds Coles: "If you can engender a culture of security, it becomes an integral part of the way the organization functions. This is one of the best and most important protections that any organization can have."

He cites an example of physical security in an oil and gas company. When Coles visited this company he was handed a safety card. The instructions included how to walk up and down the stairs. Everyone was supposed to walk up the stairs on the right side and down on the left. The handrail was to be held from underneath because this minimizes the chances of losing one's grip. "I noticed that everybody complied with this. That is just the way people walk there. If we can apply that kind of thinking to digital security and cyber security, it will become much stronger."

The most common breach for hackers is phishing, or sending fraudulent emails, which entice users to reveal sensitive information such as usernames and passwords. This allows access to personal and company data. "If we can engender a culture to not respond to unrecognized emails it could wipe out one of the main attack vectors," says Coles.

Organizations have not yet been very successful in instilling a culture of digital security. They are more focused on creating awareness through posters, videos, newsletters and the like. These measures are effective, but only in the short term, says Coles. "People tend to forget these messages after two or three months because they get consumed by their work."

"The most important part is that senior leadership and leaders down the organization must enact the values they say are important. They need to really live the culture for it to trickle down."

— Sigal Barsade

Leading by Example

So how can organizations make the shift from creating awareness to tangible behavioral change? Like so many things, culture change has to be led by the top management, says Barsade. "The most important part is that senior leadership and leaders down the organization must enact the values they say are important. They need to really live the culture for it to trickle down."

Mehta points out that in some organizations data breaches are not reported and senior managers don't worry. In others, any data breach is reported not only to the security regulator, but all the way to the top management. These behaviors depend on "how top management perceives risks and security threats." Adds Coles: "Employees are more likely to pay heed to what their bosses say and do, rather than directives from a security person they have never heard of."

It is also important to ensure that the structure of the organization is aligned with its values. Policy and procedural impediments need to be removed. Two other critical pieces are communication and participation.

Pointing out that people generally tend to hear things differently, Barsade emphasizes that "you really can't communicate enough in a culture change. You have to keep communicating." And, while typically it is the top management that decides the principal values, when it comes to executing the change, it is essential to involve people lower down. Metrics and accountability, too, need to be in place, adds Barsade.

According to Mehta, business departments must be held accountable for not only executing security initiatives but also for identifying the risks. "It is important to cover the entire lifecycle of a particular function. Ignorance cannot be excused," he says.

Understanding Mental Models

Coles and Mehta suggest that organizations need to understand the "mental models" of their employees, and how they perceive risk and security in order to influence their thinking. "If you can understand what factors different people consider when they think about risks, then you can tailor how you influence their behavior," Coles explains. "If you focus on what they think is important, then your messages are more likely to be heard and therefore be more effective."

Mehta adds that messages through examples that can translate from personal lives (backing up pictures and protecting personal banking information) to work life (backing up data or protecting client information) get understood more quickly and easily. "If you can communicate the aspects of risks in a manner that the target audience finds interesting and relevant, they will remember it and follow it."

Elements of regional and national culture also need to be factored in, especially in the case of large global firms. For instance, in many developing countries, 'tailgating' (i.e., following someone closely in a restricted area without authorization) is acceptable, while in the U.S. and Europe, it is not. "Perceptions of risk and security often vary across the world but if the corporate values are clearly defined, then it is more a matter of how you embed the change in different parts of the organization rather than the end culture itself," says Coles.

> *"You can secure anything if you think about it while developing it. Unless it is embedded early on, it becomes very difficult and costly, and it's almost impossible to get the required level of security."*
>
> — **Robert Coles**

Barsade adds that if a corporate culture value intercepts with a regional and national value, the top management has to be sensitive about how they convey and enforce the corporate culture. "They have to be thoughtful about how they get people to understand that this is how the organization will behave even if it is different from what they are used to doing."

And what role do incentives play? A significant one, says Coles, provided organizations highlight and visibly reward good behavior, and punish risky behavior. People tend to copy behaviors that they see being rewarded and avoid those they see getting punished. Barsade agrees that having rules and sanctions creates deterrents "if they are perceived as being fair and reasonable." But she emphasizes that they are not primary levers. "It's the same with rewards," she notes. "They help reinforce the value but they are not a primary lever."

She adds that one of the most consistent research findings is "that the best predictor of employee accountability is a culture of joy and 'companionate love' which means caring, compassion, tenderness and affection." Pointing out that culture change is very big and powerful but takes time, Barsade says: "A complete change can take up to three or four years because culture tends to be embedded deeply in an organization. But if companies are serious about it, they can see dramatic results even within a year."

"If you can engender a culture of security, it becomes an integral part of the way the organization functions. This is one of the best and most important protections that any organization can have."

— **Robert Coles**

This article was produced by Knowledge@Wharton, the online business journal of The Wharton School of the University of Pennsylvania. The project was sponsored by Wipro Limited.

Founded in 1881 as the first collegiate business school, the Wharton School of the University of Pennsylvania is recognized globally for intellectual leadership and ongoing innovation across every major discipline of business education. With a broad global community and one of the most published business school faculties, Wharton creates economic and social value around the world. The School has 5,000 undergraduate, MBA, executive MBA and doctoral students; more than 9,000 annual participants in executive education programs; and a powerful alumni network of 93,000 graduates.

About Knowledge@Wharton

Knowledge@Wharton is the online business analysis journal of the Wharton School of the University of Pennsylvania. The site, which is free, captures relevant knowledge generated at Wharton and beyond by offering articles and videos based on research, conferences, speakers, books and interviews with faculty and other experts on global business topics.

For more information, please visit knowledge.wharton.upenn.edu

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and Business Process Services 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 over 150,000, serving clients in 175+ cities across 6 continents.

For more information, please visit www.wipro.com