Surviving and Thriving in the Wake of a Data Breach

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity

In this article, Glenn Mott speaks with Greg Walters, Associate General Counsel for Litigation for the Peace Corps, where he provides comprehensive litigation and compliance assistance to an organization with 7,000 volunteers in 65 countries. His areas of experience include federal IT compliance law including FISMA, HIPAA, the Clinger-Cohen Act and related Office of Management and Budget guidance including Circular A-130. Greg has extensive experience developing agency risk management programs for information systems and insider threat identification and management.

NRMC: The title of your Risk Summit talk is "Cyber Survivor: Surviving and Thriving in the Wake of a Data Breach Claim." To say that 7,000 volunteers in 65 countries involve a lot of breach risks would be a gross understatement. Can you give us an overview of the Peace Corps and your daily concerns for the General Counsel's office?

GW: The Peace Corps is sometimes confused with being a private nonprofit. It is a U.S. Federal agency, yet we are very small, with a small budget, relative to our mission of bringing goodwill and friendship to the world. Nevertheless, virtually all of the laws that affect larger, domestic only agencies, such as the Department of Labor, U.S. Department of Housing, etc., we must abide by, despite having a fraction of the budgets of these cabinet level agencies. Those laws include those involving risk management and federal IT security. So we have challenges. Nevertheless, in accordance with the Peace Corps spirit, we make full use of what we have around us to solve problems.

Employee IT risk management at Peace Corps is complex—it involves four populations: 1) about 30 political appointees; 2) 1,000 federal employees (temporary members of the Foreign Service) and contractors; 3) 2,100 foreign nationals from about 60 different countries; and 4) the 7,000 plus volunteers who are not employees of the federal government—they are legally and truly volunteers, yet we provide access to health care for them. So there is a great deal of sensitive medical information available electronically and we are very concerned with HIPAA in addition to individuals' other privacy concerns.

All of these different populations use our IT network including our systems to one extent or another. Plus, they arrive at the Peace Corps with different IT security backgrounds, training, and expectations. Some federal and political employees have security clearances such as Top Secret, etc. We need to continuously manage these distinct populations with controls, training, and access. Our volunteers are wonderful and creative, but many are unfamiliar with the rules that govern what the Federal agencies can and cannot do, especially with regard to IT.

NRMC: In some organizations, individuals are responsible for ensuring compliance, but may not have the authority over the security infrastructure and implementation. Does the Peace Corps struggle in knowing when new laws and regulations exist or how to ensure compliance?

GW: What's nice about the Peace Corps and IT security, in particular, is that everyone knows each other well and works really well as a team. This includes easily sharing information about updates in the law and

regulations. We also work fast as a team—when a breach occurs, we must report to U.S. CERT (United States Computer Emergency Readiness Team) in the Department of Homeland Security. There is a form filled out and members of the breach committee are notified.

NRMC: Is there an overall manager for compliance?

GW: We have a compliance department, yes. Compliance in general at the Peace Corps includes not only federal cyber law compliance but compliance with many other federal laws and regulations. The IT security and breach aspects of compliance are the main responsibility of our agency's Chief Information Officer and especially our Chief Information Security Officer and his staff—they are the front line security team.

In addition, the Peace Corps has a Breach Committee that uses an operating manual with the subject heading: "Breach Security Response Plan." Who's on that committee is important: not just counsel, but records department employees as well. The Office of Communications and Congressional Relations are also part of the breach committee. We do our internal investigation and reporting and make sure that if something public facing is needed, everyone who is a stakeholder, such as Communications, is on board.

Nonprofits should keep in mind that when breaches occur, there is not necessarily a malevolent actor. Most breaches are inadvertent, an email sent to a wrong address, for instance.

NRMC: When people hear the words security breach, minds tend to go toward the catastrophic. What are the kinds of breaches you're dealing with on a day-to-day basis? It might be helpful to define a breach, from minor to catastrophic.

GW: Sexy sounding breaches, like that of the hackers who broke into the SEC's corporate filing database to get sensitive financial disclosures that could be used for trading aren't the rule for all breaches. Breaches that could compromise efforts at protecting volunteers and the integrity of systems will probably be more relatable to most nonprofits. The kinds of things we see at the Peace Corps include: Volunteers informally communicating with one another where unauthorized software is introduced by someone getting on the server locally and uploading files using remote access. We have people posting in 60 countries, with servers in these countries. We work with the resources we have, and much of our efforts depend upon the type of hardware the internet service providers have in use to prevent these breaches.

This is why it is key to discover the story behind the breach. We ask things like, when did it occur, the nature and means of the incident, was there unauthorized access and use of this information? There may be a lost laptop, computer list, or thumb drive, a violation or intrusion in the PC network, loss of paper documents, etc. When this happens, we look at who reported the breach, how was it discovered internally, what individuals were affected, and at what numbers. How accessible was the information? Also, was the encryption so high that a lost laptop is not an issue, or can it be shut down remotely?

NRMC: How do you close the gap between what's in the security group's purview and a disruption that requires a unified, agency-wide involvement?

GW: Closing that gap is a critical ladder in Enterprise Risk Management. IT security is the driver of this. As a government agency, we are required under federal law to have a robust program regarding IT security. This means also having very competent people at every level of the program since everyone is critical. In addition, the goal for us is to have risk management flowing from the bottom of the agency to the top, creating transparency and intelligence along its path. It doesn't depend on one exceptionally good person running the risk management program, who could leave, but rather on a continuous, established process of risk management embedded within the organization.

NRMC: What are your suggestions for bolstering security for nonprofit organizations that collect PII/SDI?

GW: Make sure there is a quick and easy way to easily report breaches. Make sure that your organization's security culture is focused on transparency first and not on initially punishing employees who innocently release protected information or accidentally upload unapproved software. It is important to discover both breaches and other IT security violations as soon as possible, and all efforts should be focused on this goal. Employees must feel that it is part of their job to report breaches.

Employees need first to understand what is protected information and how easily a reportable violation can occur before an organization can begin to move forward with a robust security plan. What isn't reported cannot be fixed. Each breach should also be a learning lesson.

NRMC: In terms of privacy and data security, can you talk about the legal requirements or necessities for nonprofits?

GW: I can't give specific advice for an organization, but generally, everyone needs to think in terms of what is the peer norm for your size/type of organization. In this world, if a legal event occurs involving privacy or data security, you do not want to be defending to anyone your organization's lack of training, awareness programs, breach reporting procedures, IT security investments, etc., when similarly sized organizations already use these tools. In addition, an Enterprise Risk Management Committee, which expressly includes IT risks, is a best practice for every organization. This ERM committee can start small, even very small, but it has a goal of providing intelligence to an organizations' leaders that may not arrive any other way. ERM analysis is expected from every federal agency regardless of its size, since there is really no other rational, defensible way for management to gauge proper investments in IT security. The Peace Corps has a formal ERM committee for all these reasons.

NRMC: We've been talking about the people, processes, technology, and culture of risk at the Peace Corps. You've also provided training to staff and outside entities on Cybersecurity training and awareness programs, gamification, and "train the trainer" type instruction designed to increase the communication skills of risk professionals. If an organization wants to review, establish, or enhance a Cybersecurity program, what are your suggestions for training and awareness?

GW: Don't make the Cybersecurity program (training, reporting, etc.) another thing that employees dread. Demonstrate the importance, and show that it's not just another way to get employees in trouble, but a way to make sure that our IT works seamlessly for everyone. Show how easily breaches occur, and how we need to be aware of these. Use stories on recent breaches by companies in the media (such as Amazon, though there are many). Show what happens when malware such as ransomware or other unauthorized software enters a network. See www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html. Websites like www.sans.org offer free security awareness materials that can be shared with staff. Make it fun—have some kind of emotional connection to the material. Use gamification techniques. Serve pizza.

I'm looking forward to seeing everyone at the Risk Summit, and hope everyone will speak about their best practices, too. There will be some gamification involved to make things fun. We'll share and keep things lively and interactive in a non-attributional setting. See you there!