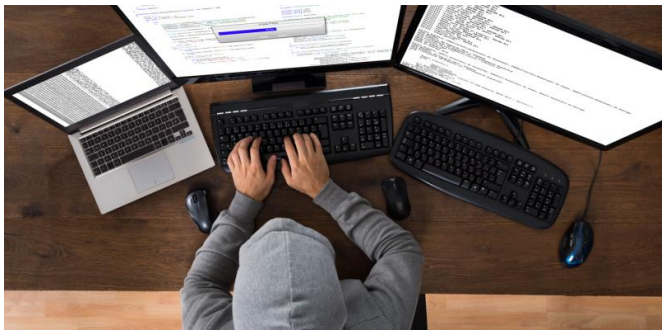
Panama Papers revelation—we must rethink data security systems

4 May 2016, by Sanjay Goel



The attacker may already be inside. Credit: shutterstock.com

The surge of information leaks from highly confidential sources in recent years demonstrates the futility of current cyber defenses.

The leaks of U.S. diplomatic cables, Office of Personnel Management data, CIA operational documents and most recently client files from the Panamanian law firm of Mossack Fonseca have created political turmoil on an international level. These dramatic breaches are confirmation that we need to fundamentally rethink our approach to data security.

Businesses and government agencies have spent much of the last two decades attempting to integrate disparate databases and information systems, seeking to improve efficiency. But that sort of consolidation is disastrous from a security point of view. It exposes vast swaths of organizational data to every intrusion, and to every insider with a password. It puts all the data on a big open field. Yes, the company builds a big wall around it all, but anyone who gets over the wall or is allowed in the door has access to everything.

Worse, the wall itself is useless. Beyond malicious insiders with broad access, other vulnerabilities render all defenses worthless. For example, "zero-day" attacks exploit previously unknown software vulnerabilities that have not yet been fixed and are not yet guarded against by security software. (The name comes from the fact that the software's authors have had zero days to address the problem.)

Social engineering attacks, on the other hand, target weaknesses in humans rather than technical tools. They use carefully crafted phone conversations or email messages to trick authorized users into clicking on malicious links or voluntarily disclosing information that bypasses security defenses.

Given all of these vulnerabilities, breaches of confidential information are inevitable. But we can limit their size and scope, and therefore their damage. Rather than building useless walls around open spaces we imagine to be secure, we must understand that the interior cannot be fully protected. Instead, we must tighten control from within, particularly by tracking all data access and usage. The goal should not be preventing the unpreventable, but rather detecting incidents quickly, and minimizing the resulting harm.

Seeking to limit damage

In the specific case of the Panama Papers, 11.5 million customer documents were copied from Mossack Fonseca and revealed to a German newspaper, Suddeutsche Zeitung, which then shared them with other news outlets as well as the International Consortium of Investigative Journalists. These revelations – 2.6 terabytes of stolen data – are a Rosetta Stone of the tax haven world. They focus on more than 3,500 people who owned shares in shell corporations that were created by Mossack Fonesca, including people with ties to 12 current or former world leaders, 143 politicians, as well as sports stars and drug lords.

While the leaker or leakers are still not identified, they may eventually be unmasked by electronic forensic work. Their points of entry, from what we know, were remarkably basic: unencrypted emails on a version of Microsoft Outlook not updated since 2009, server vulnerabilities including a WordPress plugin known to be buggy and a customer portal running on a long-outdated version of Drupal.

Simple security protocols, such as ensuring that software updates were installed regularly, would have closed these doors. While a determined attacker could have found other ways in, the treasure trove of documents now known as the Panama Papers was apparently left virtually unprotected.

Organizations should take advantage of the fact that the entire process of data extraction takes time: a hacker first creates an intrusion (or an insider first gets motivated to undertake malicious activity), then conducts reconnaissance for data access and security, and finally copies data. There is sufficient time in this process to take action that could limit damage.

Guarding from the inside

By understanding and accepting that it is impossible to create a perfectly secure computing and data environment, companies can take significant steps to increase the likelihood of timely detection, and to prevent (or at least limit) the compromise of data. They must:

1. Restrict information access based on immediate need. The push to increase productivity by integrating databases and improving data accessibility to employees has come with a security cost. Smartly controlling access to data should improve both productivity and security.
2. Log and monitor access to data and downloads, not only to enforce basic protections, but also to understand who is accessing data and why – and to record patterns of normal behavior for each user. Departures from those norms could trigger security alerts. Companies are starting to do this, but without protections that are strong enough to be really effective.
3. Divide information intelligently into separate blocks based on what data sets are really related to each other. This can prevent a single intrusion from compromising the entirety of an organization's data. For instance, people's contact information should be stored separately from records of their financial transactions.
4. Manage data archiving to regularly delete obsolete records.
5. Begin a program of active insider probes, in which security staff surreptitiously offer employees opportunities to violate access protocols, and record and analyze the responses. This can reveal malicious intentions or behavior ahead of time, and help make judgments about staff members' potential threat to become data thieves.

As individuals, we also need to conduct a personal risk analysis of the likelihood that our personal information could be leaked from companies that manage our data.

It is likely that most of the information exposed in the Panama Papers is not from criminals attempting to launder money, but rather from rich people attempting to shelter their wealth from taxes. Whether these shell corporations were designed for legitimate purposes or not, the breach has shown more than their holder's identity. It has revealed how the rich and famous hide their wealth and evade taxes. And it has redoubled suspicions about business transactions that need this cloak of secrecy.

This incident also confirms the antiquated basis of security – the overarching approach and specific programs and tools – being used in corporations today. The Panama Papers will have ongoing political, tax and business implications on an international level. With luck, they might also lead to greater scrutiny and fundamental redesigns of corporate security structures.

Source: The Conversation