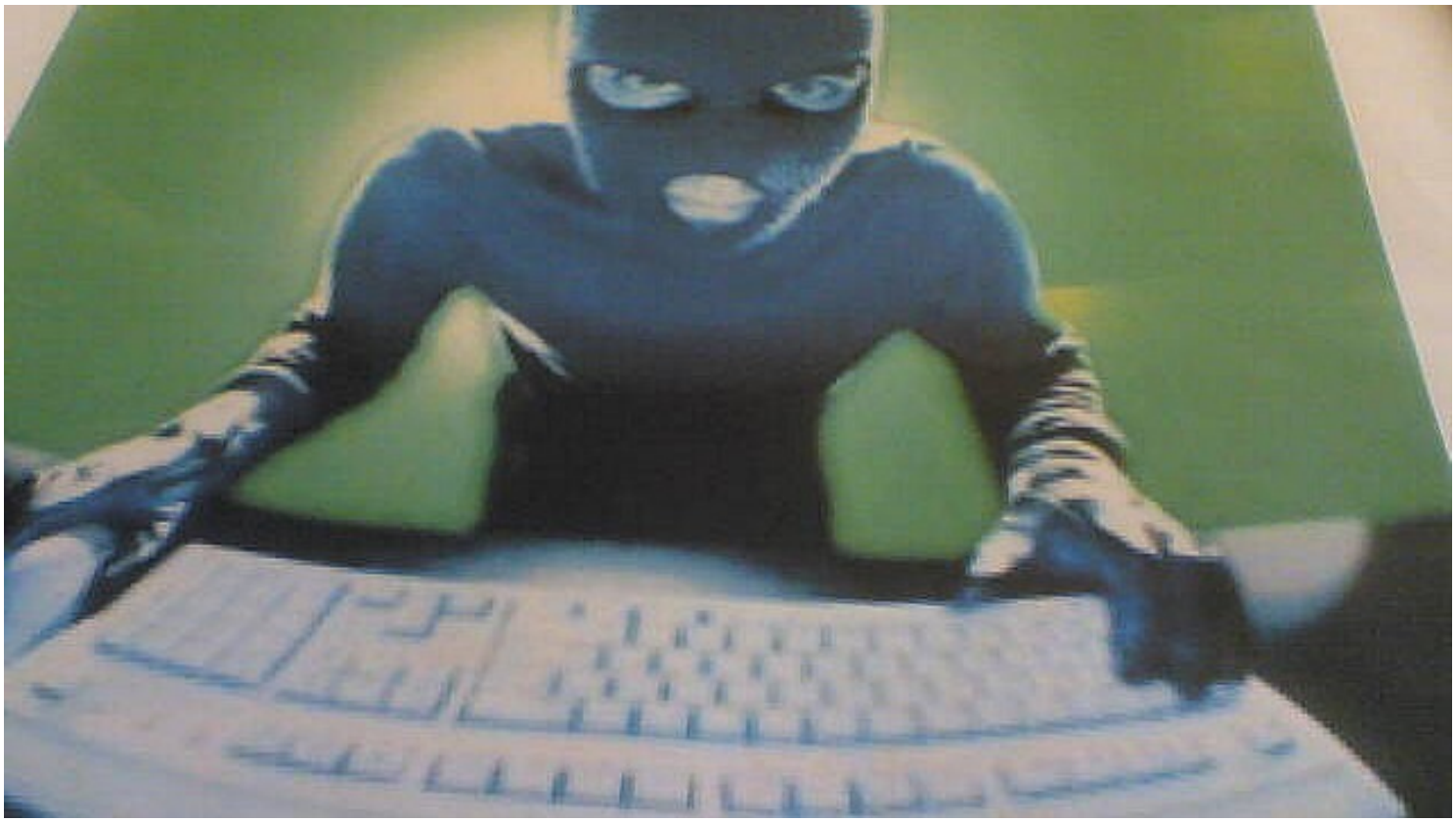
The Importance of Security Awareness in Municipal Environments



WASHINGTON, DC — With news headlines announcing major cyberattacks on a near-weekly basis, it's likely that most people realize hackers and cyber criminals pose a significant threat, overall. However, with the media focusing on "mega breaches," smaller entities such as municipalities may assume they aren't likely targets. After all, hackers want the most bang for their bucks, right?

In reality, the answer is "Not necessarily." Although some criminals attack major sources of sensitive data, such as the card-payment records of giant retailers, many others have realized that smaller entities are just as attractive. Furthermore, security breaches aren't limited to broad-based hacker attacks. Careless employee behavior is a leading source of data leakage.

In many cases, a data breach results from someone capitalizing on an opportunity, not taking an overt action. In this article, we'll explain why municipalities are vulnerable and offer practical, affordable suggestions for defending against these threats.

The Smaller, the Better?

To illustrate the mindset of cyber criminals, consider armed robbers. Although a major heist is appealing, it's often safer and easier to hit a handful of poorly guarded banks or stores rather than go after one big score. The same is true for hackers and other cyber villains.

Initially, the world saw this principle in action with businesses. Hackers first went after big corporations but later turned to smaller targets. Today, the U.S. Department of Homeland Security reports that 31 percent of all cyberattacks are directed at businesses with fewer than 250 employees.

With governments increasingly on the hot seat, many experts predict that municipalities and their agencies will become even more attractive. While it's difficult to pinpoint the percentage of cyberattacks leveraged at cities because they are not well represented in surveys, it is indisputable that cyber criminals are targeting them and have been doing so for years.

In 2011, the media reported that the online hacker group Anonymous had broken into 70 rural law enforcement computer systems, defacing websites and exposing sensitive information. Fast forward to the present day (March 2015), and the FBI reports it is investigating a cyberattack on the city of Madison, Wisconsin, in which hackers blocked or interrupted official communications including email and some police and fire dispatch services. The cyberattack was similar to those that have occurred in other cities after officer-involved shootings. In between these two events, there have been numerous incidences of municipalities and their agencies being cyber attacked, either to steal data, disrupt city services or extort ransom for hijacked digital assets.

Becoming a Victim

Municipalities are attractive to hackers for the same reason that small businesses are appealing—they are often inadequately protected. After the Anonymous hack, the National Association of State Chief Information Officers (NASCIO) announced that 50 percent of states report they spent less than three percent of their IT budgets on security. In our experience working with municipalities around the country, this figure is still largely accurate.

Yet, municipalities often present much more attractive targets to cyber criminals than their size might indicate. One reason is that they store an amount of personal data disproportionate to their size. Few small businesses have 25,000 customer records, for example, but a city of only 5,000 households might have that many personally identifiable records—often including payment information—among its property tax, business tax, public works and other systems. Thanks to transparency initiatives and small budgets, this data is often not secured with the diligence that a similar cache of sensitive information would be, elsewhere.

Cities also control municipal systems that hackers increasingly exploit, such as water treatment plants and energy plants. Cities that don't have sufficiently large utility systems to make them targets are often tied into larger grids, making them prime entrance points for criminal activities.

Power of the People

So, what can a city do to protect itself and its citizens from cyber criminals? While the value of sophisticated security hardware and platforms cannot be underestimated, the single most common "vulnerability" in any system—digital or physical—is the human element. (One study, by IBM, found that human error or poor decision making was the culprit behind 95 percent of security incidents.)

Unlike computers, people don't function logically. They have an unfounded amount of confidence in their own decision-making ability and an unreasonable level of faith in the familiar. These traits may have served humans well when they were hunting mastodons or seeking shelter during tribal wars, but they are extremely dangerous in a digital era. Unfortunately, despite their "mission" of serving the people, government employees are no exception to this rule.

Examples of human error causing cyber-damage in governments are legion. One of the largest data breaches (at the time) occurred in 2012 at the South Carolina Department of Revenue. In this instance, an employee responding to a malicious email inadvertently exposed the private data of 3.3 million bank accounts, 3.8 million taxpayers, 1.9 million dependents and 699,900 businesses.

For municipalities with only a few servers, an entire towns' worth of records could be exposed by a single employee responding to a malicious email or browsing to an infected website. Given that many cities connect with the databases of other local, state and federal agencies, such a mistake could eventually have a broad, negative impact across multiple levels of government.

Taking Corrective Action

Now that we have sufficiently alerted you (we hope), let's discuss fixing the problem. Before we do, I want to reiterate one absolute fact. ***It is impossible to alter human nature. However, it is entirely possible to teach humans how to avoid their own impulses.*** Just as children learn early on that fire will burn them, computer users must have knowledge of the dangers of their own carelessness ingrained into their behavior patterns. Then, cities must support that learning externally, as well. Here are a few suggestions:

1. **Take Precautions:** Implement security measures, such as browser helpers, that scan for infected sites and communications and warn users not to proceed. (This is an important start, but it isn't enough. Numerous studies show a percentage of users will click on a link even after being told it is infected.)
2. **Train by Example:** A fundamental component of security education is training people not to make foolish mistakes. Training can take the form of classes on security and reference manuals, including teaching keywords frequently used in malicious emails, (Order and Payment are the top two).

   However, we recommend including exercises as part of the training effort. Returning to the fire example, above, burning oneself is always more effective than being told to avoid a flame. For example, some firms create fake "infected" messages from an unfamiliar email account and send them to employees as a test. Employee that click on the link are transported to a company site that informs them they could have been hacked.

3. **Enact Stringent Policies:** Municipalities should create and enforce stringent policies regarding computer activities such as personal browsing on city networks. Those who are caught breaking the rules should be punished—including eventual termination if the behavior continues. (These programs must be properly structured and documented to protect the city from retaliatory action.)
4. **Lock Down Access:** People cannot expose what they cannot access. Governments in particular are known for being far too permissive regarding personnel data privileges, including the ability to post personal information to public-access sites. IT providers can perform network assessments that identify devices on the network (including rogue or unauthorized devices), explore permissions and perform other investigative tasks to help initiate this effort.
5. **Keep Systems Updated or Take Them off the Network:** Tight budgets are unavoidable, but updates and patch application are crucial to security. If a municipality cannot afford to upgrade all of its computers to current-generation operating systems and keep them properly updated, they should restructure their computer allocations to shift outdated (e.g. Windows Vista or older) computers off the main municipal network. These machines can still be valuable for training or other non-networked activities.
6. **Protect Mobile Workers:** Lost laptops, notebooks and mobile devices are culprits in the "human error" statistic cited earlier. Municipalities should implement mobile device management programs, including remote locate, lock and wipe services, for all devices that leave city offices.
7. **Give Something Back:** If a city has a public-access network separate from their internal one, it could set up a few computers in a break room or other area where workers can access the Internet during free time. It is a fact that even the most diligent employee may break the rules regarding digital access if they are not given a legal means for checking personal email, social media and other platforms during the day.

A Staged Approach

As we mentioned earlier, municipalities should also deploy firewalls and other security appliances to protect their departments and data, even if they have to perform the work in stages. With or without those protections, the steps outlined above are also very valuable and they result in less financial strain. The assessment mentioned in item #3 is an inexpensive way to help city officials determine further, needed action.

Author Bio

Neil Matchan, Chief Technology Officer, InterDev

After joining InterDev in 1998 as a Senior Systems Engineer, Neil Matchan rose through the ranks to become Director of IT Services (2006-2013) and in 2014, Chief Technology Officer (CTO). As CTO, Matchan has been instrumental in developing, managing and growing InterDev's Managed Services program. Matchan studied Industrial Psychology at Georgia State University and graduated from the Network Administrator Specialist program at Oglethorpe University.

The following two tabs change content below.

- Bio
- Latest Posts

Neil Matchan

After joining InterDev in 1998 as a Senior Systems Engineer, Neil Matchan rose through the ranks to become Director of IT Services (2006-2013) and in 2014, Chief Technology Officer (CTO). As CTO, Matchan has been instrumental in developing, managing and growing InterDev's Managed Services program. Matchan studied Industrial Psychology at Georgia State University and graduated from the Network Administrator Specialist program at Oglethorpe University.