Darryl Booth, MBA

Building Capacity by Guarding Against Cyber Attacks

Editor's Note: A need exists within environmental health agencies to increase their capacity to perform in an environment of diminishing resources. With limited resources and increasing demands, we need to seek new approaches to the business of environmental health. Acutely aware of these challenges, the National Environmental Health Association (NEHA) has initiated a partnership with Accela called Building Capacity—a joint effort to educate, reinforce, and build upon successes within the profession using technology to improve efficiency and extend the impact of environmental health agencies.

The *Journal* is pleased to publish this column from Accela that will provide readers with insight into the Building Capacity initiative, as well as be a conduit for fostering the capacity building of environmental health agencies across the country. The conclusions of this column are those of the author(s) and do not necessarily represent the views of NEHA.

Darryl Booth is the general manager of environmental health at Accela and has been monitoring regulatory and data tracking needs of agencies across the U.S. for almost 20 years. He serves as technical advisor to NEHA's informatics and technology section.

Phishing, distributed denial-of-service, and ransomware. These are three modes of criminal attack that can devastate an organization. Girding your health department for these and related attacks is as important as preparing for any other disaster—it is an element of emergency preparedness.

Phishing

Phishing is a deceitful attempt to obtain information (e.g., account details) by e-mail, text, or the Internet designed to impersonate a legitimate request. So, what appears to be an e-mail from the county help desk, for example, asking to confirm your contact information is, in fact, an enticement to give up your username and password to a third party.

The oddly spelled word phishing comes from the hacker propensity to replace the letter "f" with "ph" in deference to 1970s telephone system hacking, a practice known as phreaking. The reference to fishing is easily understood if you think of an ocean of potential victims (fish) attracted to fancy colorful lures. Fishing.

The Threat

With stolen credentials, perpetrators could gain unauthorized access. With that access, they might retrieve protected information, change data, or wait silently. That is, the credentials might be sold (yes, there's a market for stolen credentials) or used to gain access to increasingly sensitive systems (the true target).

For environmental health, the attack is a threat to privacy and ongoing operations.

The Defense

Like most emerging threats, educating users is the best defense. For example, if your bank seemingly invites you to access your account with a convenient hyperlink, close the e-mail and navigate to your bank's website directly.

Other clues include misspelled words, off-brand language and/or images, and URLs (i.e., web addresses) that don't match the expected website.

Using security configuration to allow privileges to those needed by each user also reduces risk. Gaining access to a limited account isn't as catastrophic.

Top-tier security experts, such as those employed by major cloud-based providers, will also defend against and monitor for intruders.

Distributed Denial-of-Service

Distributed denial-of-service (DDoS) is a coordinated attack on your network from the outside world. Inconceivably, the attack can involve hundreds of thousands of attackers, computers previously compromised and instructed remotely to generate constant network traffic all bound for your network.

So, while your health department's website or e-mail servers respond to normal requests (e.g., to send a web page or receive an e-mail) at a certain level, they are not equipped to handle millions of requests each hour. The illegitimate traffic floods out the legitimate requests, denying the service it is intended to provide. Think about trying to talk to your date during a loud Rolling Stones concert. Your communications can't get through!

The Threat

Thankfully, this type of attack is not the fault of any single user within the department. This type of attack might arise from a political or revenge motivated incident. It's external.

During an attack that can go on for hours or days until blocked or abandoned, certain network services could be unavailable or intermittent. Those services can include the agency's website, e-mail server, and virtual private network (VPN).

The Defense

Responsibility for monitoring and responding to this type of attack lies solely with your agency's information technology organization/department and its tools and vendors. Any threat of this nature should be taken seriously and the health department, an essential service, should receive full attention after emergency response services. Get those assurances.

Having a distributed environment (i.e., critical applications are hosted in the cloud and noncritical applications are maintained in the county's data center) will preserve critical services during an attack.

Ransomware

Often injected into an organization by a phishing scam, ransom malware or ransomware takes compromised computer systems and methodically encrypts the organization's files, both local and on network file servers.

When the encrypted files are no longer accessible and the organization is crippled, an e-mail—a ransom note—is sent that demands a fee (often to be paid in Bitcoin, an anonymous payment method on the Internet) to unencrypt (unscramble) your files.

Search no further than today's headlines to see the impact on networks the like of Cooke County, Texas; the City of Knoxville; and the Texas Department of Transportation. Government agencies are very often the victims with some paying the ransom and others rebuilding from backups. In the most devastated cases, the attack becomes a matter of public debate and requires the Federal Bureau of Investigation to investigate. Many more cases are never reported.

Image courtesy of iStockphoto, AKodisinghe.

The Threat

Encrypted files are simply inaccessible, garbled by an essentially unbreakable code. Without the files, the critical systems on your network will be inaccessible. No posting financial transactions. No dispatching inspectors. No running state reports. No payroll!

Also, while the encrypted files are "under the control" of the hacker, they can be read or copied. So, beyond the inaccessibility that can last days or weeks, there is a high risk that sensitive data are compromised.

The Defense

Since most ransomware is delivered through phishing, protection starts with anti-phishing systems and education.

Keep operating systems up-to-date and restrict the ability to install software to administrators. Antivirus software can prevent attacks in some cases. Also, the data systems hosted in the cloud are almost always protected. While ransomware runs rampant in local networks, it cannot access the cloud-based systems in other networks. The bottom line is to be confident in your backups and your vendors. Make it automatic and frequent for the best protection.

Building and Protecting Your Capacity

Building capacity is the topic of this column. Like environmental health programs that surveil and intervene, the most successful outcomes are the absence of an event. That is, avoiding a security breach is similar to preventing a foodborne illness in many ways. Intent, consistency, and education are key.

As environmental health leaders, you might not perceive that cyber security is among your responsibilities. Consider, however, that circumstances that threaten to disrupt your essential mission are relevant and worthy of your attention.

Corresponding Author: Darryl Booth, General Manager, Environmental Health, Accela, 2633 Camino Ramon #500, San Ramon, CA 94583.
E-mail: dbooth@accela.com.

Did You Know?

You can view NEHA's Digital Defense: Education for a Safer World Virtual Conference & Exhibition on-demand until February 28, 2021. The free, on-demand offering includes access to the recorded Food Safety and Water educational sessions and the Exhibition and Poster Halls. Learn more at www.neha.org/digital-defense.