FINLEY ENGINEERING
INTEGRITY INTO EVERYTHING

STRATEGIES TO IMPROVE CYBERSECURITY

BACKGROUND

According to a 2013 survey of power and utility company executives by EY (formerly Ernst & Young), only 11 percent of respondents reported feeling that their current data security measures fully met their needs. In addition, 60 percent of respondents reported that they were running no, or just informal, threat assessments. And, 64 percent agreed with the statement that their security strategy "is not aligned with today's risk environment."

Such a scenario is problematic in and of itself. However, it is even more problematic when one considers that 80 percent of the respondents noted that they had witnessed an increase in external threats, such as malware and phishing.

In commenting on the report, Fraser Nichol, director of EY's Information Security practice, noted, "A more proactive approach, greater employee awareness, innovative security solutions, and an integrated information security programme will enhance a company's defenses against inevitable cyber attacks and protect it from potential reputational damage, regulatory action and higher costs."

CYBERSECURITY THREATS

"When it comes to hacking, the hackers often don't care what they are hacking - an electric utility, a phone company, or anything else," said Laren Metcalf, Director, IP Services, for Finley Engineering (St. Louis Park, Minn.). "For a lot of them, it's a 'glory attack' - just trying to show they can do something and then brag about it." Of course, the most serious attacks are the targeted ones - those that are malicious and are designed to "mine out" data, financial, business, and/or personal.

"The ones we are seeing the most of are 'denial of service' attacks," said Metcalf. In these attacks, "bots," which are remote programs on different systems, are deployed, allowing the hackers to gain control of the systems. In many cases, the users don't even know their systems are being controlled. "This type of attack involves going into a network and repeatedly making requests to systems for acknowledgement of service. Ultimately, all of these requests can't be fulfilled, because there are so many coming in," he said. As a result, the systems either fill up trying to track all of these outside connections, or they reboot or fail due to the inability to keep up with the requests. Larger provider networks have systems that are built to handle this, or offload the traffic, so they can maintain some level of service. However, in the smaller networks, it can become a major problem, ultimately cutting service.

There are also NTP (network time protocol) server attacks. A request comes in for information or data. "Here, you are not only dealing with a 'denial of service' attack, but massive amounts of data are trying to be sent back to the requester, which immediately locks up the service," said Metcalf.

STRATEGIES TO IMPROVE CYBERSECURITY

"Security is critical for utilities, because they provide essential services," he said. If there are attacks, there are disruptions of critical services, as well as legal issues, such as failing to meet regulatory and other compliance requirements. These days, though, just having a firewall and anti-virus software on your system isn't enough anymore.

The first step to addressing cybersecurity issues, according to Metcalf, involves focusing on employee behavior in terms of how they interact on the Internet. This can be done through training. "For example, if employees receive suspicious e-mails, they should be trained not to click on them," he said.

The next step is to arrange for a cybersecurity assessment, via a formal audit, conducted by an experienced third party. Such an audit will identify possible areas where security is lax. Having an outside firm conduct the audit is important, because someone from the outside who has worked on these issues before can provide a lot more insights than you will have on your own, as well as being updated on the most current attacks and other vulnerabilities, and the solutions to these.

Such an audit should cover everything end to end, not just systems that the utility thinks are the only important ones. "For example, an audit can identify systems on the network that haven't been identified as critical, but, if a hacker can gain access to them, they can load something on there," said Metcalf.

In addition, an audit should identify systems that aren't up to date. For example, patches are being offered these days to solve intrusion problems. If you apply these patches, you have some protection. However, a lot of users don't bother to apply new patches. "Hackers can exploit this," he said. Once a patch is released and publicized, the hackers identify it and begin to exploit it. Then, the users who haven't done the security updates and applied the patches become targets.

A good audit will also use probes as a way to monitor the type of traffic that is on the network and identify a distribution of the most common types of traffic that you have, and whether these are valid.

Overall, an audit involves identifying all of a network's systems, tracking them, and identifying what is needed to make sure they are up to date on security protection initiatives. "The most important thing to remember is that, if you can identify a risk, you can mitigate it," said Metcalf. "A comprehensive audit will identify all of these risks. It will identify everything on your network and how it is set up, where the systems are connecting on the network, and what access they have."

The audit should also include the creation of a formal cybersecurity policy, which will include information on who in the organization will have access to what.

Once the audit is complete, the results should become part of your day to day operations. "For example, any time you have a project, there will automatically be a security component to it that must be addressed," he said.

Is there a need for third-party cybersecurity expertise after an initial audit? Yes. For example, you should call in the outside firm when you are not sure of something and feel you need an outside expert to help you address it, such as a recent incident. You should also call in the expert when there is a change in your network, such as adding a new service or new location with new users. Finally, it can be a good idea to arrange for short, quarterly update audits, to make sure your cybersecurity program continues to run smoothly and effectively.