



Utility Reduces Security Risks With Thorough Assessment

Reliability and security are cornerstones of the utility industry.

But as the grid becomes intelligent, it can also become susceptible to cyber attacks that can damage operational integrity. And utilities need to be prepared. For a mid-Atlantic utility, preparation took the form of security consulting services from Verizon aimed at a hardened security posture and operational compliance with NERC CIP standards.

Specifically, the company realized they needed to get a handle on their electronic perimeter, as well as a generation management system (GMS) application. Satisfying these needs began with a thorough current-state assessment of the network infrastructure, including both administrative and grid components, as well as mission-critical energy management applications.

Security today pays dividends tomorrow.

We found a number of software applications with vulnerabilities. Further investigation revealed that the problem was much more than a few tactical programs. Assessments discovered that the company needed to train their developers around secure coding so they could start incorporating security from the outset, rather than making expensive coding repairs late in the software development lifecycle.

With Verizon on retainer, they were able to quickly schedule our security experts for a secure coding training class with 25 developers. This included several days in the classroom to go through our best practices training on security coding methodology, with a particular focus on the GMS energy platform. In addition, we provided training on security monitoring and fine-tuned a third-party security logging platform. Now—through a “train-the-trainer” approach—the company has the in-house expertise to build hacker protection into the development stages of their applications.

We have more than 1,200 security professionals in 30 countries supporting a range of professional services and managed security solutions that help you address the challenges of your extended environment.

Crime doesn't pay, but understanding it does.

Although information technology calls for a specific knowledge and skill set, other aspects of security often call for a more creative approach: thinking like a criminal. That's where the social engineering aspect of security enters the picture, and it's an area that carries significant risk. Employees must understand and execute their role in tightened security.

The utility asked us to assess their security procedures, and we found reason for their concern. Through a number of targeted calls to contact center employees, a slim majority divulged login credentials to internal websites and the corporate network. We also found that more than 50 percent of these

The Verizon Cybertrust Security Solution provided:

- Application security assessments
- Improved security practices in application development lifecycle
- Understanding of network segmentation and security
- Business partner security reviews
- Voice over IP (VoIP) security assessments in preparation for VOIP implementation
- Employee security awareness and secure code development training

Ask the Right Questions to Find the Best Solutions

It is good security practice to perform periodic, broad, third-party security assessments. The first step in achieving up-to-date, hardened security is to determine existing vulnerabilities. The findings help form strategic mitigation plans for both funding and building a plan of action to protect your enterprise.

Our examination helped the utility answer:

- Are we investing our security budget properly to block or close potential entry points that can result in compromise?
- Are we protecting data properly if an attacker were to compromise systems?
- Are shared administrative user credentials used properly so that access doesn't lead to compromised applications or data?



employees would provide access credentials when requested by a phony website set up for the investigation. Armed with this information, we advised the company on security best practices for personnel.

Wireless is everywhere, but is security?

Wireless network access is ubiquitous, but good security controls against intrusion aren't. That led to scrutiny of this operational component as well, as part of our governance, risk, and compliance consulting. Although the infrastructure itself was solid, rogue wireless access points were a big concern. We looked at seven locations, including service centers and operational facilities. We physically walked down certain sites to discover rogue devices and vulnerabilities, and found misconfigured wireless computers allowing entry and rogue access points without security controls, some of which could be used for illicitly entering the corporate network.

Our wireless vulnerability assessment provided the awareness and our consultants provided the expertise needed to quickly and effectively address these potential routes to data and operational compromise.

After a broad enterprise security assessment, the company leveraged our expertise to further harden its security posture and achieve NERC CIP compliance.

To achieve tight security, be proactive.

Security, like housework, is never done. Conditions change, and security must keep pace. As this mid-Atlantic utility continues to evolve operations, efficiencies, and partnerships, they will continue to rely on our security expertise, including 15 years experience assessing risk, and designing, implementing, and managing security solutions.

For our Investigative Response (IR) services, the utility can call upon us for onsite evidence collection, electronic data recovery, computer forensics analysis, and litigation support, among other services.

Our retainer contract makes it easy to engage us. With one call we immediately begin to tackle the issue. And that includes broader security services such as enterprise-wide or application vulnerability assessments, and consulting around areas such as logging platforms and architecture support.

As we move forward, we are working to help the utility with business partner and vendor connectivity reviews, realizing that up to 40 percent of breaches come from business partner connections. Why? Too often, the relationship with the partner and its benefits receive the majority of the focus, at the expense of careful examination of partner or vendor security practices and potential vulnerabilities. We'll help the utility proactively address the issue and realize that partnerships entered without due diligence can bring security risks.

Finally, as the utility looks to add the efficiency of voice over IP (VoIP) to its operations, they will begin with a Verizon security assessment of potential security concerns. It's another example of the transition to a more proactive approach to security, because the best security means being one step ahead of potential threats. With Verizon, the utility is moving its security to the head of the class and keeping it in line with regulations—and that means maintaining both physical and virtual operational integrity.

Learn more about our Energy and Utility solutions at verizonbusiness.com/solutions/utility and b2b.vzw.com/industrysolutions/utilities.html.

About Verizon Business

Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.

verizonbusiness.com

verizonbusiness.com/socialmedia verizonbusiness.com/thinkforward

© 2010 Verizon. All Rights Reserved. CA14627 7/10
The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

