SECOND SIGHT SYSTEMS

Total Solutions
Provider for Industrial &
Utility Communications

The Alarming Numbers Behind Utilities' Cyber Threat

While the Internet of Things (IoT) has brought us more data and efficiency, it has no doubt created new vulnerabilities. Everyday, hackers and malicious software target energy, water, and other critical infrastructure providers, seizing confidential information and invading control systems. Despite advanced security firewalls, threats are on the rise, leaving operators ill-confident in their ability to mitigate high-impact risks.

If there is one challenge facing critical infrastructure the most, it's the urgent need to protect systems against internal and external threats, with a focus on worse-case scenario and high-impact attacks. The following is a look at the shocking number of incidents, the level of readiness, and the impact cyber risks pose to utilities and other infrastructure providers. Whether we're talking about the number of incidents or the financial toll of potential attacks, the cyber threat is real, and demands a multi-level response.

RISKS

4.37

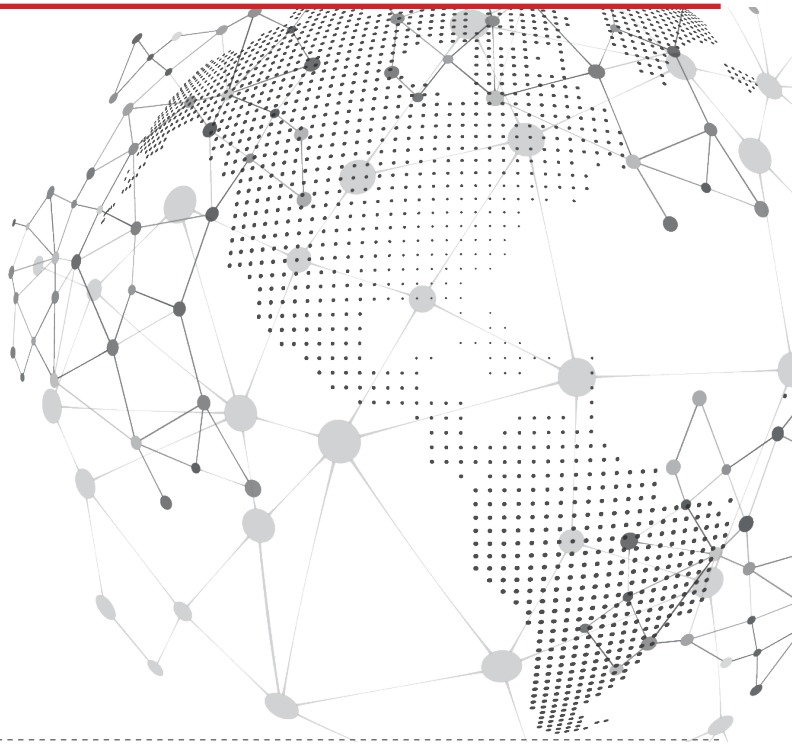
is the ranking U.S. utilities gave cyber security on a scale from **1-to-5 of importance,** making cyber risks the second most important issue for electricity providers after grid reliability. [1]

64,199

cyber security incidents occurred across **82 countries** and **20 industries** in 2015. [2]

2,260

cyber breaches, with **confirmed data loss,** took place worldwide in 2015. [2]



70%

of the world's power, water, and critical infrastructure providers reported a breach in the past year, which led to **a loss of confidential information or a disruption in operations.** At the same time, 78% of providers expected a successful breach of their ICS/SCADA systems within the next 2 years. [3]

295

critical infrastructure incidents were reported by U.S. companies in 2015, **up from 245 in 2014.** Critical manufacturing was the most hacked sector in 2015 with nearly 100 incidents reported, followed by the energy sector with 46 reported incidents, water with 25 incidents, transportation systems with 23 incidents, and government facilities with 23 incidents. Many more incidents go unreported. [4]

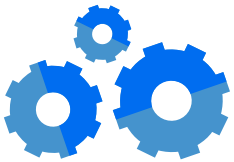
12%

of these incidents (35 incidents) resulted in an intrusion into the company's control system, **up from 9%** in 2014. [4]

Top 5 Security Threats

Insider negligence, system glitches, denial-of-service attacks, malicious or criminal insiders, and third-party mistakes are the main security threats to U.S. utility & energy companies.[5] In fact, accidents are nearly 50% of the root cause of security breaches in ICS/SCADA systems, while external attacks made up nearly 30% of breaches. Current and former employers were behind nearly 70% of breaches, compared to hackers which made up 18%.[5]

READINESS



70%

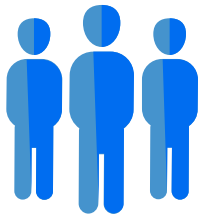
of utilities and energy sector companies have a deployed an **IT security strategy,** yet many lack a plan to protect its operational technology (OT). 46% are unsure if their organization can effectively manage security risks to critical assets. [5]

50%

of energy sector organizations said they have sufficient resources to achieve compliance with security standards and regulatory requirements. But less than 10% have a department dedicated to **ICS/ SCADA security,** and only a third have adopted or plan to integrate the NIST cybersecurity framework.[5]

56%

of the organizations indicated they are lacking in real-time actionable **cyber security intelligence,** which is critical to emergency response. [5]

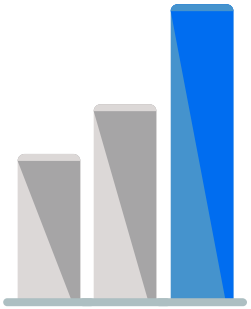


209,000

unfilled cyber security jobs are needed in the U.S., with **job postings up 74%** in the last 5 years. [6]

$12.61 BILLION

is the projected spend on ICS security in 2021, **up from $7.82 billion** in 2014. [7]



IMPACT

$243 BILLION TO $1 TRILLION

is the estimated **economic loss** if the most damaging scenario of a widespread cyber attack on the U.S. power grid occurs. [8]

$2.4 MILLION

is the amount Lansing, Michigan's Board of Water & Light invested to develop a **cyber-emergency response** after doling out a $25,000 ransom to cyber criminals in 2016. The utility's insurance covered the bulk of the expense. [9]

700,000

people in the Ukraine went **without power** in December 2015 after a well-known trojan called Black Energy attacked the electric grid. [10]

SOLUTIONS

Second Sight Systems is a market leader in providing secure solutions to critical infrastructure. We recognize that cyber risks are here to stay and will increase over time. To effectively defend control systems, it's imperative that utilities add controls to protect critical systems, install more effective monitoring, and develop an emergency response plan. Adhering to revised NERC, NIST and ISC-CERT guidelines are key step in this process. Utilities need to adopt a continuous and proactive approach that addresses IT/OT convergence and goes beyond avoiding or responding to security breaches, but rather, generates a system-wide resilience against cyber threats. With new federal regulation and industry willingness to adopt new security measures, a better, more secure grid is possible.

SOURCES

1. Black & Veatch: 2016 Strategic Directions: U.S. Electric Industry
2. Verizon 2016 Data Breach Investigations Report
3. Security Week: Unisys & Ponemon Institute 2014 Survey
4. Security Intelligence: ICS-CERT Reports 2015 Infrastructure Attacks
5. Scottmadden: 2015 Energy Industry Cyber Security Report
6. Cyber Security Jobs: Bureau of Labor Statistics, Forbes Report
7. ISC Market Projections
8. Lloyds of London Findings, Utility Dive 2016 Report
9. Cyber Attack on BWL, 2016 Report
10. Ukraine attack, 2016 Zdnet Report

SECOND SIGHT SYSTEMS