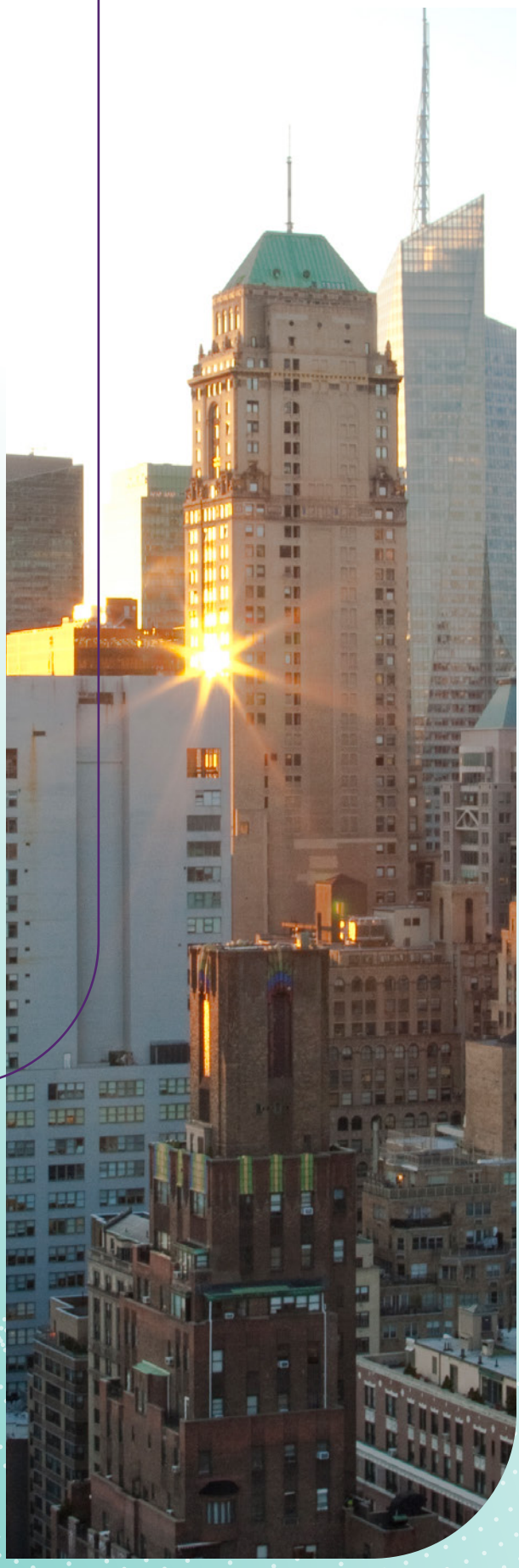
FROM INVESTMENT TO IMPACT: HOW UTILITIES CAN OPTIMIZE VALUE FROM OT SECURITY PLATFORM INVESTMENTS

1898 & Co. PART OF BURNS & MCDONNELL | UTILITY DIVE

Custom content for 1898 & Co. by studioID



Utility leaders have extraordinarily full plates. From rapid load growth to the difficulties of maintaining reliability in the face of increasingly extreme weather, utilities must navigate unprecedented challenges and opportunities.

Adding to the challenges is the reality that they are under continuous assault by increasingly sophisticated cybercriminals. Indeed, when compared to the previous year, cyberattacks on utilities increased by 70% in 2024. According to the Federal Bureau of Investigation (FBI), many of the attacks are being launched by foreign nations, including China, which FBI Director Christopher Wray said was preparing to "cause real-world harm to American citizens and communities"

Cyberattacks on utilities increased by 70% in 2024

Utility leaders have responded to the growing frequency and sophistication of cyberattacks with a range of investments to protect the grid and other utility infrastructure, complying with regulations like the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. Many utilities have invested in operational technology (OT) tools, such as intrusion detection and prevention systems, asset discovery, threat detection, and firewalls provided by companies like Dragos, Nozomi Networks, and Claroty.

Investments in OT security platforms are a powerful first step towards enhanced cybersecurity. "What these platforms can do is identify the weak spots of these networks, and they can effectively give information about how to limit the impacts," said Mark Mattei, 1898 & Co. global director of industrial managed security services (MSS) and incident response. "Utilities are making great strides by implementing these risk reduction efforts. These platforms don't guarantee you're not going to get hit. But if you use them properly, you can have greater resiliency."

To better understand both the cyber threats utilities face and the return on investment that OT security tools are delivering, 1898 & Co. and Utility Dive's studioID surveyed over 100 utility industry professionals. Respondents represented a broad swath of the industry, with about half working at natural gas utilities, one-third from electric utilities, and the remainder from water utilities, independent power producers (IPPs), independent system operators (ISOs) and regional transmission organizations (RTOs). Those who responded to the survey were in leadership positions, with about 40% at C-level — including CEOs, CFOs, CISOs and CIOs — and the remainder at the vice president or director level.

"Utilities are making great strides by implementing these risk reduction efforts. These platforms don't guarantee you're not going to get hit. But if you use them properly, you can have greater resiliency."

MARK MATTEI
Director, Industrial Cybersecurity
Managed Security Services, 1898 & Co.

SURVEY SAYS: UTILITIES NOT GETTING FULL VALUE FROM OT SECURITY TOOLS

Several common themes emerged from survey responses. Indeed, the survey clearly shows that utility industry leaders understand the elevated risk of cyberattacks and that many companies have already suffered the consequences of successful attacks.

In fact, despite being a heavily regulated industry with growing cybersecurity compliance obligations, over half of the respondents have already been victimized by cybercriminals. And many of the attacks had meaningfully negative impacts on the companies, including:

More than **50%** of respondents said a cyberattack resulted in an inability to deliver services.

36% of survey respondents lost revenue in the aftermath of a cyberattack.

As the risk of cyberattacks grows, so too does the understanding among utility leaders about what is needed to bolster their prevention and response capabilities. In fact, 95% of utilities said that greater visibility and situational awareness would improve their cyberattack detection and response time.

95% of utilities said that greater visibility and situational awareness would improve their cyberattack detection and response time.

The survey also clarified that traditional information technology (IT) cyber defenses were insufficient to protect utility OT assets. Indeed, 76% of respondents said that IT cyber defense tool sets were not sufficient in an OT ecosystem. Furthermore, 95% of utility leaders reported having already deployed or were considering the deployment of an OT security platform. However, the survey did not clarify exactly how respondents defined an OT security platform. "Respondents say they have OT security, but they might just have a firewall," Mattei said. "They may say they have OT security because they have firewalls in their OT environment. But it may not be the full scope of tools for threat detection and vulnerability mitigation and all the things you need for holistic OT security."

95% of survey respondents identified real-time network monitoring as a priority.

Regardless of what utilities believe constitutes an OT security platform, there are clear priorities in what leaders want the tools to deliver. At the top of the list is real-time network monitoring, which 95% of survey respondents identified as a priority. Other OT security platform functions deemed "very important" by survey respondents included:

- Attack surface management (59%).
- Incident response (54%).
- Threat detection (52%).
- Asset discovery (49%).

Both the outcomes and the capabilities utilities want from the significant investments they make in OT security platforms are understandable. The increased risk of successful cyberattacks and the negative financial, operational, reputational and regulatory impacts they can impose demand a robust and effective response.

However, the main takeaway from the survey is that, while an essential first step, investing in an OT security platform is not enough on its own to deliver the outcomes utilities expect and require. In fact, 30% of survey respondents reported that their OT security platform vendor either falls short or, even worse, "greatly" falls short in supporting their utility's needs. Additionally, 43% of companies said they receive either moderate or "very few" benefits from their OT security platform.

A PEOPLE PROBLEM

The survey raises an important question: Why are so many utilities not getting the full value of their investments in OT security platforms? For many in the industry, it's fundamentally a people problem.

For example, about one-third of survey respondents said that one of the main challenges to receiving the full benefits of their OT security platform was a lack of in-house expertise. The lack of expertise within utilities helps explain why nearly 20% of respondents said they had insufficient confidence in their vendor, and another 36% complained that platform complexity was a barrier to enhanced cybersecurity.

Over half of the survey respondents said they couldn't find qualified candidates to staff an OT-centric cybersecurity team. Some utilities have responded to this reliance on vendors by educating and training internal teams. But this approach has its own risks. Utilities may not have the capacity to train staff properly, and even if they do, it can be difficult to retain people after they have been trained.

Over half of the survey respondents said they couldn't find qualified candidates to staff an OT-centric cybersecurity team

An alternative approach is to enlist the help of managed security service provider (MSSP) professionals with the skills and expertise to ensure utilities receive the maximum benefits of their OT security platforms. This step can deliver benefits beyond the expert management of OT security platforms.

"MSSPs elevate the maturity of cybersecurity beyond just the specific service provided," said Keith Walsh, an MSS cybersecurity principal for 1898 & Co. "For example, threat detection has second and third-order effects of mitigation and risk reduction from finding configuration vulnerabilities. And continual attack surface monitoring helps shorten the gap closure time for attackers to take advantage of new vulnerabilities."

Though not explicitly addressed in the research, another challenge limits utilities' capacity to leverage OT security platforms fully and underscores the benefits of working with an MSSP. Regulatory pressures are limiting utilities and increasing their dependence on complex on-premise solutions for OT cybersecurity. "Utilities aren't happy with their on-premise solutions and they need people to manage it because it is so complex and difficult," Walsh said. "As NERC-CIP grapples with CIP 4 and 11, these utilities are beholden to on-premise offerings, which data tells us falls short due to staffing issues. Until NERC-CIP evolves to accept SaaS (software as a service), utilities can solve the people issue by working with a firm like 1898 & Co. that combines service-oriented offerings with deep industry knowledge"

"Utilities aren't happy with their on-premise solutions and they need people to manage it because it is so complex and difficult."

KEITH WALSH
MSS Cybersecurity Principal,
1898 & Co.

NEXT STEPS TO SECURE THE FULL VALUE OF AN OT SECURITY PLATFORM

Getting the full return on investment (ROI) from OT security platforms depends on having the right people and resources to guide their optimal use. As the survey highlighted, that expertise does not yet exist at most utilities.

Unfortunately, utilities can't expect vendors to supply the expertise needed to get the most out of the platforms. "We're in a trough of disillusionment right now where these utilities are still getting hit by cyberattacks, and either nobody is managing their own environment, or they left, or they're not trained properly," Walsh said. "If utilities look to their platform vendor, the vendor says they are not staffed to provide you enhanced services, even if you want to pay for it."

Given the financial, operational, regulatory and reputational risks a successful cyberattack poses, not fully leveraging the capabilities of an OT security platform is not a viable option. For most utilities — but especially small and medium-sized firms — hiring an OT-focused MSSP for threat detection and response is a more efficient and effective option than finding, training and retaining internal staff. MSSPs deliver specialized expertise, advanced tools, around-the-clock monitoring, and cost efficiencies that most utilities can't replicate internally. Working with an MSSP allows utilities to focus on their core mission of delivering reliable and secure power.

The choice of an MSSP, then, becomes critical for utilities to defend their OT assets properly. Utilities should that insist any potential MSSP is able to offer:

- **Specialized expertise in OT security.** An MSSP should have deep knowledge and experience with a wide range of OT protocols, including Modbus, DNP3 and OPC-UA, which differ significantly from IT protocols. MSSPs should also have meaningful experience with industrial control systems (ICS), particularly supervisory control and data acquisition (SCADA) systems. Additionally, the ideal MSSP will be equally well-versed in both IT and OT security tools to ensure they work seamlessly to complement one another.

- **Cost-effective access to advanced tools.** Powerful and comprehensive OT-specific threat detection tools can be prohibitively expensive for utilities to acquire, optimize, operate, and maintain in-house. Utilities should prioritize working with MSSPs that can deliver the benefits of advanced tools at an affordable price.

- **Talent.** Finding, training and retaining combined OT and cyber expertise is a challenge for utilities. Doing this in-house adds significant cost, which can be difficult for utility leaders to justify. An MSSP must be able to provide expert and experienced personnel to ensure you get the most out of your OT security platform.

- **Rapid incident response and proactive threat hunting.** One way to evaluate an MSSP is by assessing whether it can provide the fundamental capabilities that result in greater cybersecurity. For instance, does the MSSP have dedicated teams equipped with proven playbooks to respond to incidents? Is it an expert in proactive threat-hunting techniques that identify vulnerabilities before they morph into meaningful threats?

Ideally, a utility will bring an MSSP on board early in the process of selecting an OT security platform. "That way, it's possible to get help with the architecting and configuration of the tool," Mattei said. "We come into a lot of environments where tools are already implemented, which is fine. But coming in and helping the client pick the right tool to get the best return on investment based on their architecture is ideal so we can better configure and tune that specific tool for your environment."

Another benefit of partnering with an MSSP in the selection of a platform is that it means the MSSP can then be accountable for its performance. "We can have consultative discussions around the specific outcomes that they want," Walsh said. "That helps inform which platform to choose because not all tools are created equal. But if we are involved in the selection of the right tool and its configuration and operation, then we can be held accountable for the outcomes."

There are big differences in what different MSSPs can deliver. For example, because 1898 & Co. is part of Burns & McDonnell, it can tap unrivaled experience and expertise in critical infrastructure. "We have the capability to draw on the vast range of knowledge from our employee owners across the U.S. and around the world who have spent their entire careers building, architecting and engineering the assets we are now protecting," Mattei said. "That means I can grab the person who built the asset during an emergency incident response and clearly understand the way they architected and engineered the OT network."

"We have the capability to draw on the vast range of knowledge from our employee owners across the U.S. and around the world who have spent their entire careers building, architecting and engineering the assets we are now protecting."

MARK MATTEI
Director, Industrial Cybersecurity
Managed Security Services, 1898 & Co.

1898 & CO.®

PART OF BURNS McDONNELL

1898 & Co. is a leading consulting firm serving critical infrastructure clients who keep our world in motion. Part of Burns & McDonnell, our experience and foresight converge to manage risk, identify opportunities, leverage data and navigate digital transformation. We're engineering- centered business consultants who understand the complexities of your business and deliver practical solutions that fuel future growth, drive smarter decisions and maximize value. Learn more at 1898andCo.com.

Learn More

studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more