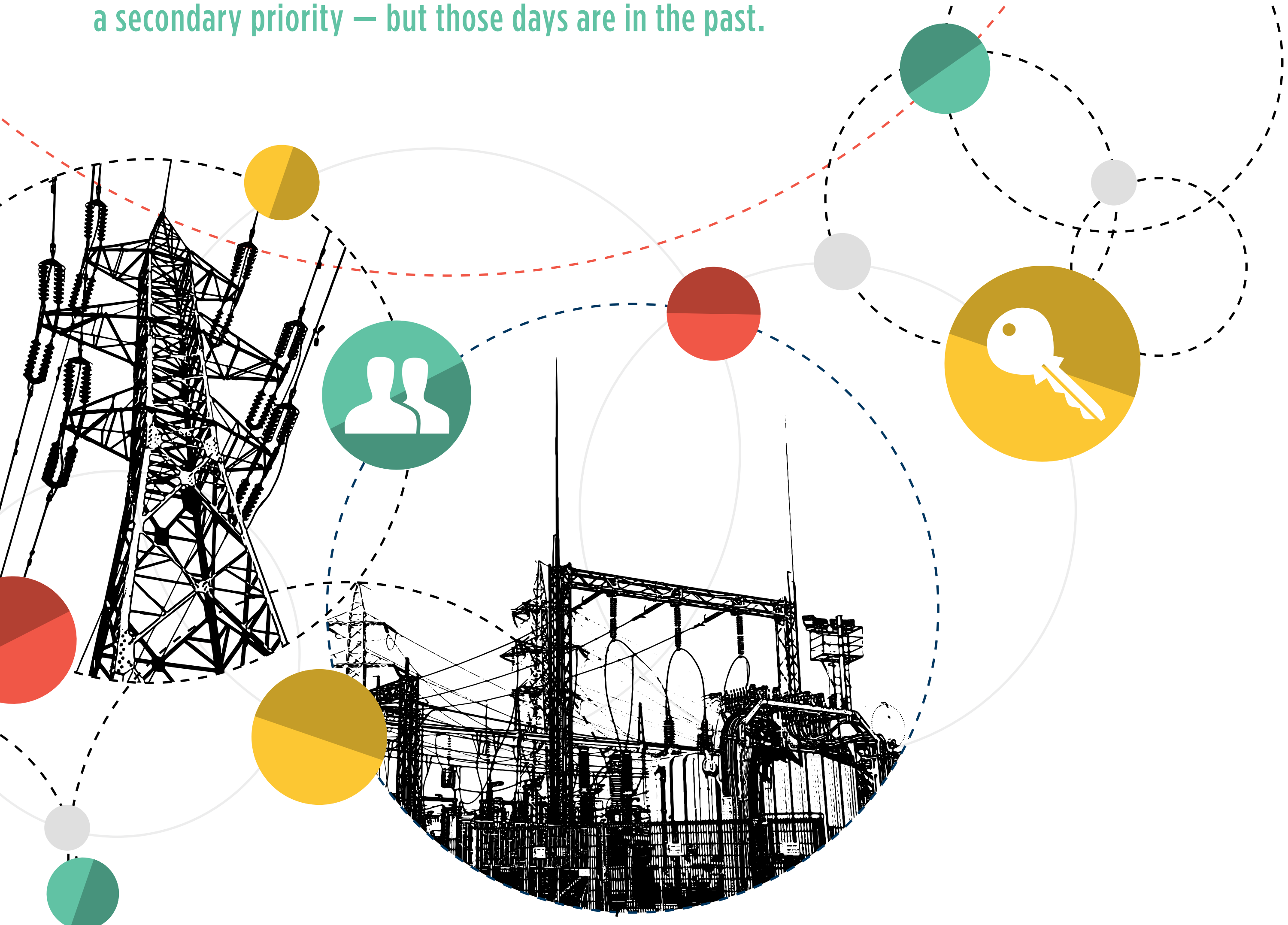
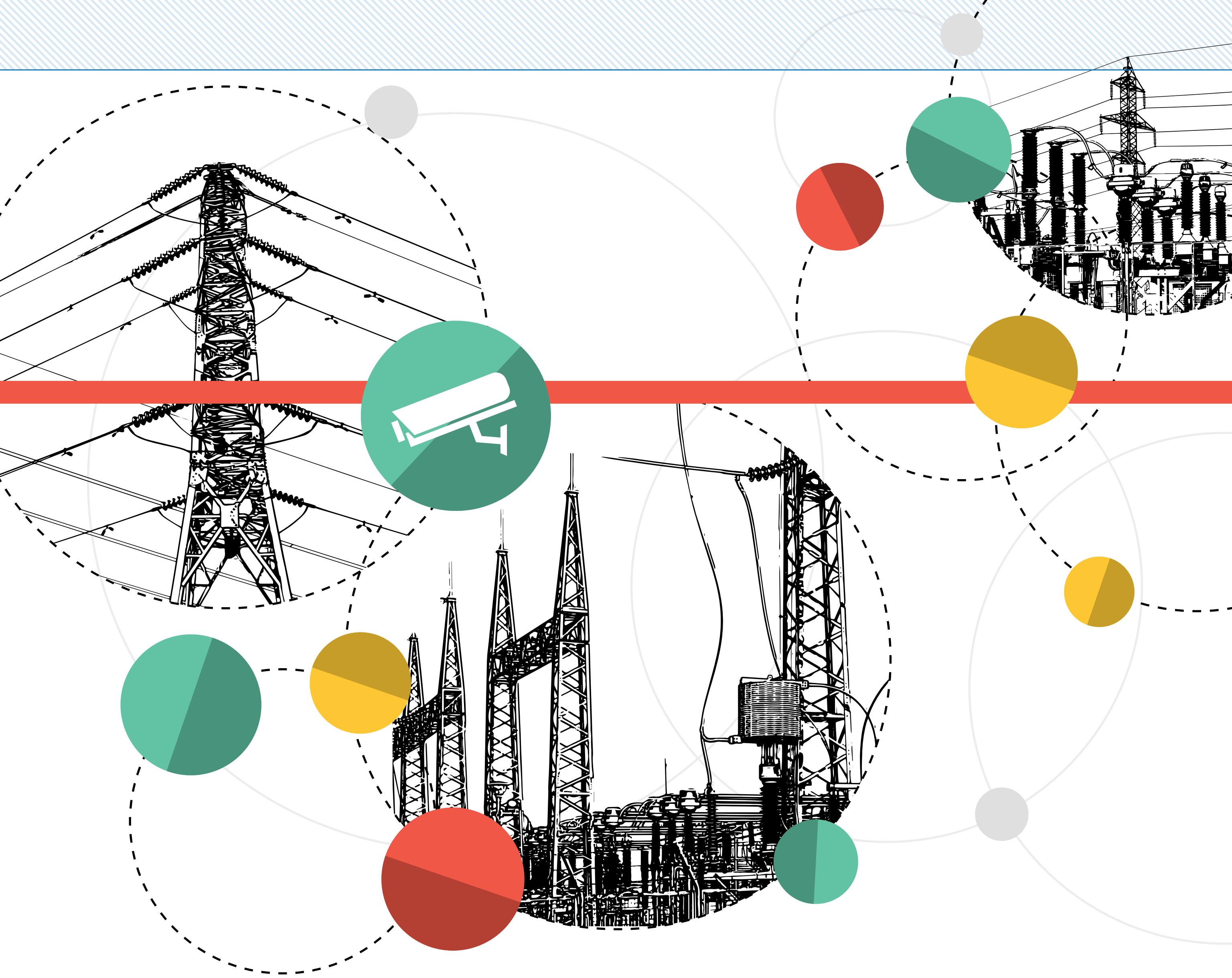
# INTERCONNECT

## TO SECURE AND PROTECT

As recently as a decade ago, electric utilities often considered an integrated physical and cybersecurity plan a secondary priority — but those days are in the past.





As the electric grid moves steadily in the direction of "internet of things" operations, it's becoming increasingly vulnerable — especially to cyberattacks.

"The issue now is not 'if' utilities are integrating these security measures. It's how best to assess, select and deploy these solutions across their supply chain," says Jerome Farquharson, regional manager of compliance and critical information protection at Burns & McDonnell. He points to increased threats, more interconnected systems and large fines of noncompliance as contributors to this shift.

Because of these amplified risk profiles, the number of third-party vendors offering security solutions has proliferated, flooding the market with technologies that often accomplish the same things in different ways. This can make it difficult to select and implement the most effective systems.

"Before, utilities may have had a handful of choices for surveillance or intrusion detection," Farquharson says. "Now, they have dozens of options for every single element. It can feel overwhelming."

Identifying best-of-breed point solutions and bringing them in-house has become an industry trend. But Kevin Fuller, who leads the security services group at Burns & McDonnell, says utilities are finding this approach can result in too many tools with too much overlap.

"Consolidating tools around a holistic security program is becoming a priority," Fuller says. "Then the real challenge for a utility becomes understanding its greatest priorities before investing in additional technologies." »

# STEPS FOR A SOLID SECURITY PROGRAM

An integrated plan helps utilities make smart capital investments and operations and maintenance expenditures, meet regulatory needs, bring all stakeholders onboard and — ultimately and vitally — reduce security vulnerabilities. These tips provide a framework for success.

## 01 Take it back to basics.

It’s not unusual to see a utility with five enterprise resource planning (ERP) systems — none of which correlate — and 20 different spreadsheets tracking assets. That can result in a lack of understanding of internal security processes and how well they work.

“Before adding another solution, work to get your house in order,” says Keegan Odle, director of substation projects at Burns & McDonnell. “It’s not glamorous, and it’s time-consuming, but a program’s success is dependent on this first step.”

## 02 Find appropriate partners for holistic planning.

A thorough process demands significant effort and coordination among a wide variety of stakeholders, typically across departments. And funding often comes from different sources: the information technology department, the transmission group and the infrastructure fund, among others. An experienced security consultant with working knowledge of the power industry can unite efforts.

## 03 Assess the risks.

Benchmark and conduct a maturity assessment using known evaluation frameworks.

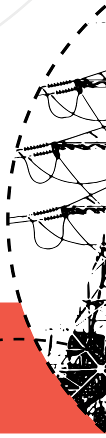
“Organizations all have blind spots,” Fuller says. “An external view can identify gaps, regulatory or otherwise. Road map what prioritization needs to occur against these risk profiles and how they will be implemented.”

He encourages utilities to put security standards in place as a requirement for suppliers and vendors.

## 04 Develop a checklist and share it internally.

A checklist of necessary security values should become a much-used document.

“Spend a lot of time establishing exactly what’s needed,” Odle says. “Create a great action plan, make sure it’s scalable, and share it with all affected stakeholders — from operations and maintenance to construction and community outreach.” Every vendor should demonstrate how a technology meets this criteria.



For a closer look at substation perimeter security — including compliance with NERC CIP-014 — check out **burnsmcd.com/DefendingTheEdge**.

## 05 Leverage current relationships.

A utility's existing technology providers typically have a vested interest in a successful outcome — and a better understanding of current processes and patterns.

"Before shopping around, show your current providers your requirements and ask if they can meet them," Farquharson says. "A utility may be able to drive a vendor's development to a new place."

## 06 Check in with your peers.

If a utility still finds gaps after leveraging current relationships, it might find the answer with an industry peer. Utilities on the cutting edge of specific technologies are often willing to share lessons learned and best practices. The increasing urgency behind security efforts can lead to a heads-down approach, so it's important to look around, see what's been done and share knowledge.

## 07 Consider new tech.

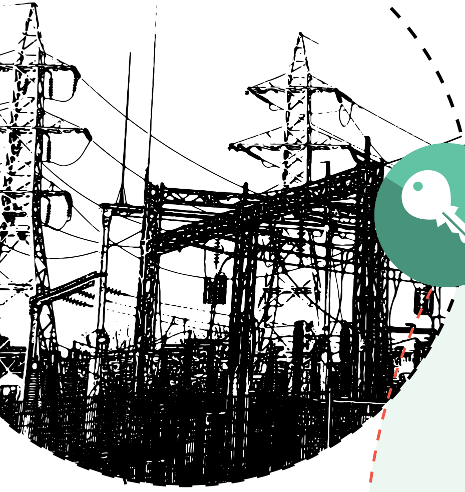
For each new technology, utilities should consider their evolving needs, along with business requirements and training implications. Farquharson suggests establishing how well a new tool can integrate into current processes so users can adapt in the shortest amount of time. He also emphasizes customer references as part of the decision-making process.

"Any solution a vendor tries to sell has already been sold, unless you are the test dummy for that particular product," he says. "In that case, get a financial incentive during negotiations for playing that role."

## 08 Test, measure and refine during implementation.

A phased approach that prioritizes stakeholder buy-in is a smart choice, regardless of specific technology. Ongoing program testing with a reusable, real-life scenario is a valuable tool for rollouts, pilots, ongoing updates and evaluations of future products.

"Eventually, utilities can move to an assurance model because they've built a culture of checks and balances," Farquharson says. "And measurement should be a constant. Are performance goals on track? If there is a breach, how quickly could your organization identify and respond? The best security programs are based on constant improvement."



## LET STRATEGY BE A GUIDEPOST

In the utility industry, physical and cybersecurity planning has come a long way. Integrating security elements is now an essential part of the typical design approach rather than an afterthought. The increasingly competitive product landscape drives vendors toward more efficient solutions. But even as security technology zooms into the future, a security program built on smart and methodical strategy will serve as a guidepost.

"Security capabilities change quickly because the tactics the adversary uses change quickly," says Kevin Fuller, security services leader at Burns & McDonnell. "But don't let the speed of evolution paralyze your efforts. There is never one magic bullet. As long as a utility has clarity on what's important, it'll have the capability to successfully match the appropriate technology solutions."