

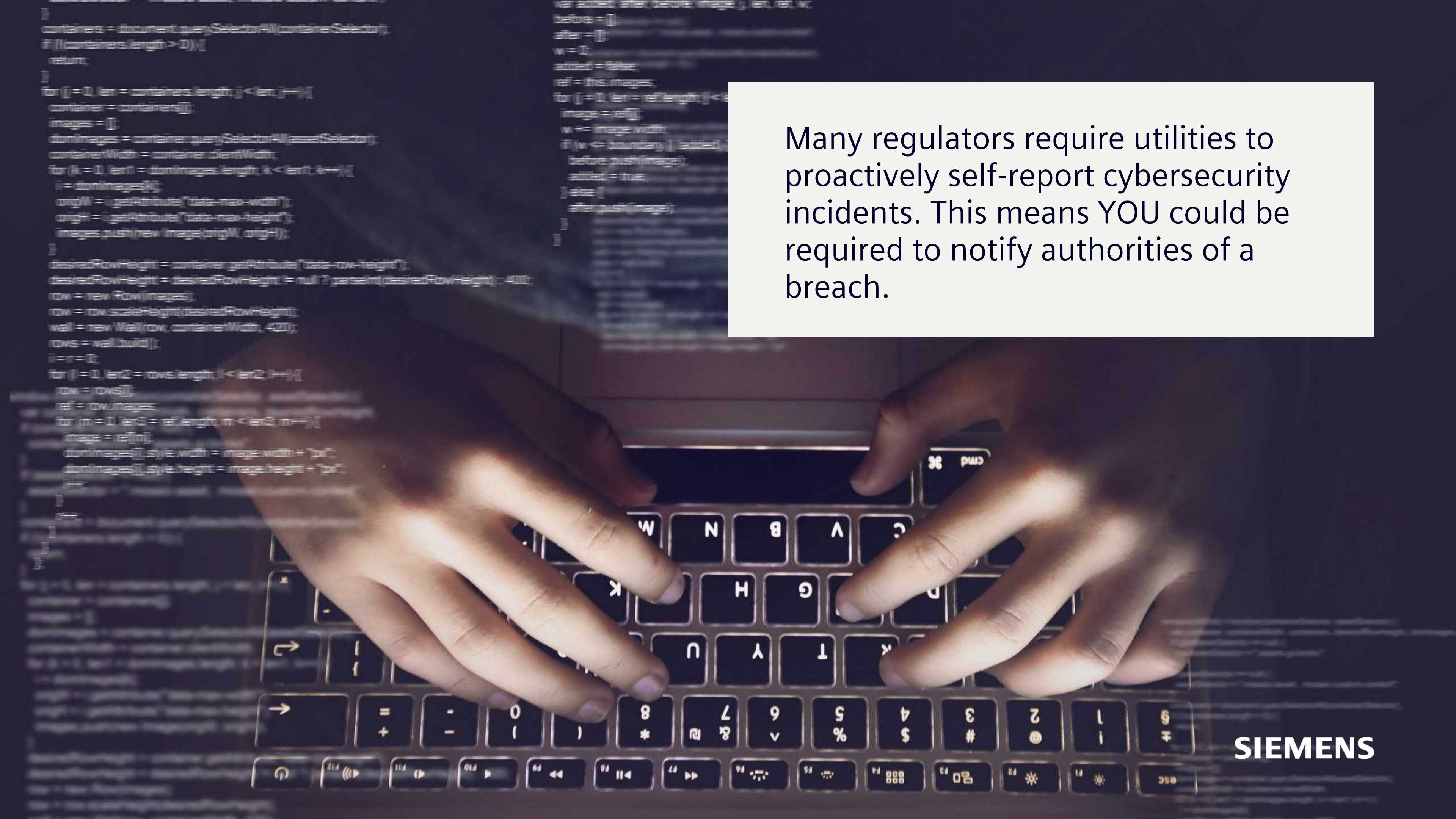


**Because government
regulators mean business**

SIEMENS


**When government
regulators come calling,**
particularly during and/or
after a cybersecurity event...
they mean business.

SIEMENS

A close-up photograph of a person's hands typing on a laptop keyboard. The background is a dark, out-of-focus screen displaying lines of code in a light-colored font. The lighting is warm, highlighting the keys and the person's fingers.

Many regulators require utilities to proactively self-report cybersecurity incidents. This means YOU could be required to notify authorities of a breach.

SIEMENS

A man with a beard, wearing a white button-down shirt, is seated at a wooden desk in an office. He is looking down at a laptop screen, with his right hand covering his face in a gesture of stress or frustration. The desk is cluttered with various items: a laptop, a small potted plant, a coffee cup, and some papers. In the background, there are several other computer monitors and office equipment, suggesting a busy work environment. A dark blue rectangular box with white text is overlaid on the right side of the image.

Regardless of who initiates the conversation, compliance audits aren't fun. And if you're not prepared, it can be costly.

SIEMENS

Beyond putting public safety at severe risk,

the consequences for utility operators not being ready for cybersecurity related audits can be significant. The Executive Order issued in 2020, now makes it a requirement that your systems be designed to be “un-hackable.”



A close-up photograph of a hand in a light blue shirt sleeve, pointing the index finger downwards. The hand is the central focus of the left side of the image.

Non-compliance with NERC-CIP regulations could mean:

- Steep fines for your business
- Diversion of precious time/resources to fix what went wrong
- Potentially long-term reputational damage to your company
- Possible negative impacts on your personal reputation and/or career

IIoT and digitalization have brought many benefits to the power industry. But achieving this added value has also meant **greater scope and security coverage in your NERC CIP Procedures, Implementation Plans, and Maintenance Programs.**

COMPLIANCE

RULES

STANDARDS

POLICIES

SIEMENS

Here are 5 steps
you can take to boost
your confidence level
for that next audit.

SIEMENS

Step 1:

Make smart choices when selecting your equipment. Choose products with the right technology and protocols built in.

SIEMENS

Step 2:

Partner with a company who has a distinct focus on OT communication networks and the unique needs of power utilities and NERC CIP regulatory requirements.



WE UNDERSTAND
YOUR NEEDS

SIEMENS

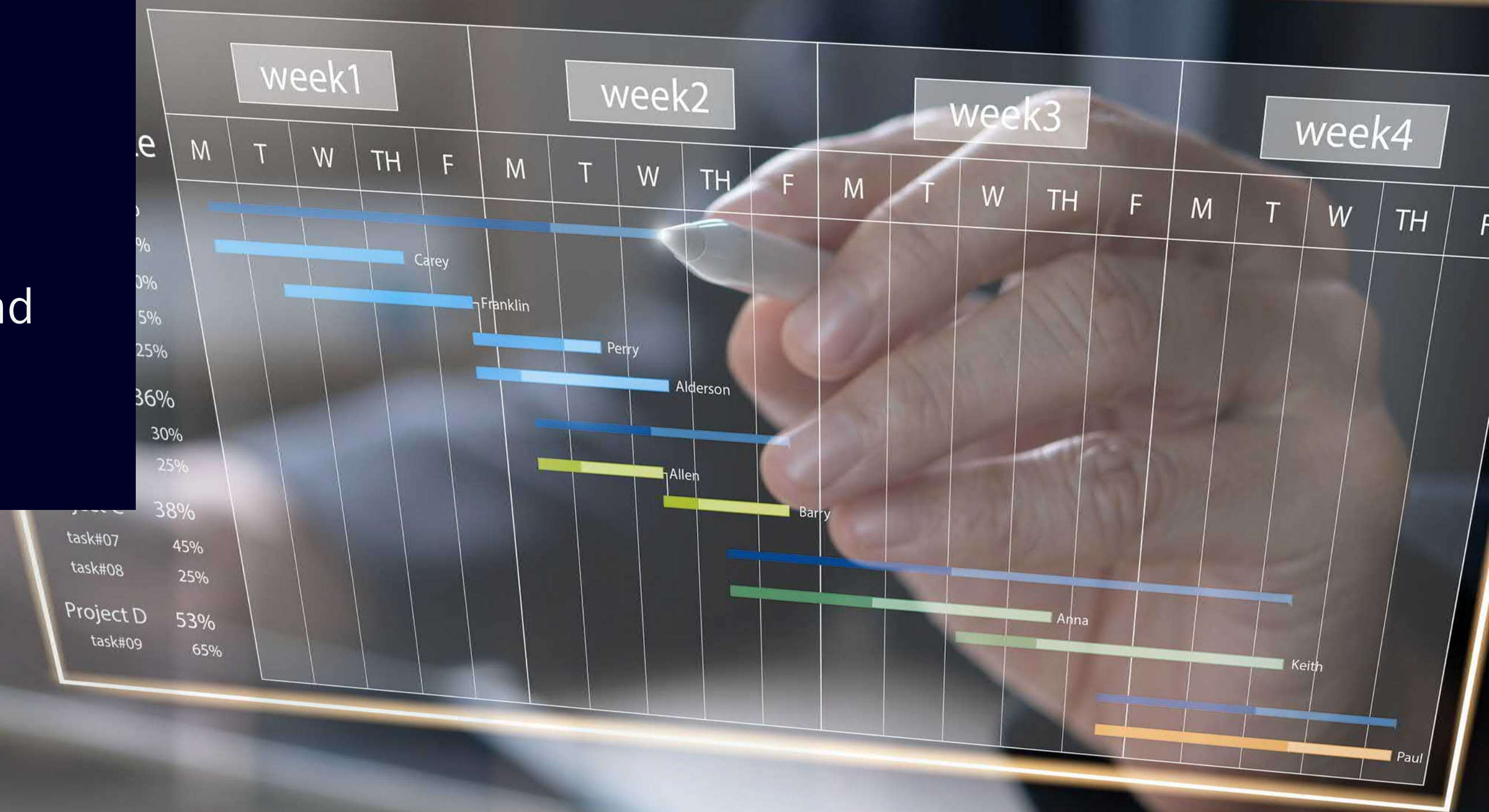
Step 3:

Routinely conduct a comprehensive cybersecurity assessment to identify potential system vulnerabilities. Strive for:

- Clear remediation recommendations
- Consistent communication security
- High levels of operational integrity

Step 4:

Set a course to optimize your communication networks' capabilities and cybersecurity.




Step 5:

Update your Implementation and Maintenance Plans, while addressing the training needs of your staff. The success of any plan rests on those charged with maintaining it.



SIEMENS

A photograph of four professionals in an industrial setting, likely a power plant or substation. They are wearing hard hats and safety vests. Two men are holding laptops, and a woman is holding a tablet. They appear to be engaged in a discussion or inspection. The background shows large industrial structures and power lines under a clear blue sky.

As the global leader for industrial communication networks, Siemens is the trusted partner for leading utilities, with deep expertise in power system requirements and the ability to help utilities stay out of regulatory crosshairs.

SIEMENS



Our RUGGEDCOM hardware and software are designed around NERC-CIP requirements and incorporate “Open Systems Architecture” to make sure our systems evolve to best-in-class standards for decades.

SIEMENS


Our Network Services Team assists utilities with designing future-proof and secure networks. This is key when employee bandwidth is low and when technology is outpacing corporate training program capabilities.



SIEMENS

Our services include:

- Network Health Checks + Cybersecurity Assessments
- Network Design Consultation + Implementation
- Hardware and Software Pre-configuration and Testing
- Embedded Engineers for large project implementations
- Network Certifications + Custom Training – Onsite and Virtual



Benefit from our multi-service platform, and our certified cybersecurity partners. We consult with you to implement “the right solution in the right place” for full network protection including:

- Anomaly-based Intrusion Detection System (IDS)
- Deep Packet Inspection (DPI)
- Next Generation Firewall (NGFW)
- Intrusion Prevention System (IPS)

Address secure device and remote access through our RUGGEDCOM CROSSBOW solution. With administrator-defined Role Based Access (RBA), CROSSBOW provides activity logging and data privacy as users connect to remote Intelligent Electronic Devices (IEDs).

The background is a blue-toned image featuring a hand holding a small electronic device. Overlaid on this are several semi-transparent gears of different sizes. Various white icons are placed within or around these gears: a cloud with a signal line, a fingerprint, a laptop, a smartphone, a padlock, a network diagram, and a server rack.

SIEMENS



**CROSSBOW is NERC CIP
compliant and feature rich:**

- Strong two-factor authentication through RSA SecureID, ActiveDirectory + RADIUS.
- Automated functionality for device password management, configuration, firmware version monitoring, remote connectivity.
- Customizable reporting (i.e. SCADA vs Real Time Reporting; Engineering vs Compliance; Inventory and Configurable Alarming reports).
- Includes data file retrieval so you are ready with the details regulators require.

Contact us today,

and take the first step in
boosting your confidence
for your next audit, and
protecting your:

- Network
- Brand
- Business
- Career
- Customers

with Siemens'
RUGGEDCOM solutions.

siemensci.us@siemens.com



SIEMENS

RUGGEDCOM

Because Rugged is more than our name.

SIEMENS

SIEMENS

usa.siemens.com/ruggedcom