# Is the Cyber-Security Threat to the Electric Utility Industry Real?

NDEQ Power Summit 2018

Tim Pospisil, Director of Corporate Security & Chief Security Officer

October 30, 2018

Nebraska Public Power District

*Always there when you need us*

# Topics for Today

- Nation State Threats
- Supply Chain Threats
- Business Email Compromise (BEC)
- What Can You Do?

TLP:WHITE

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

HIRT | HUNT & INCIDENT RESPONSE TEAM

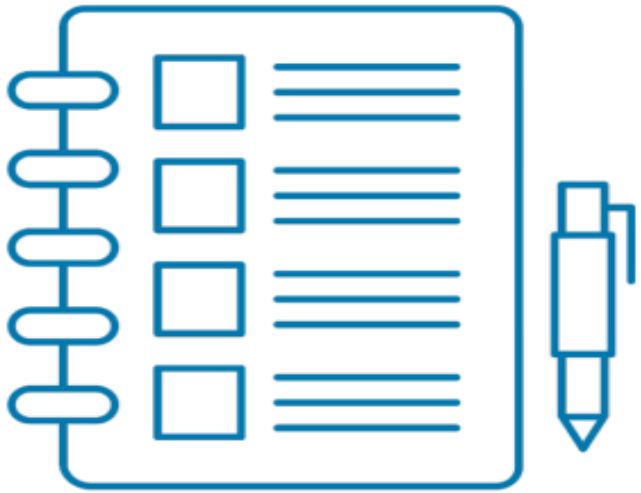
# RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE

NCCIC

TLP:WHITE

TLP:WHITE

# Campaign Summary

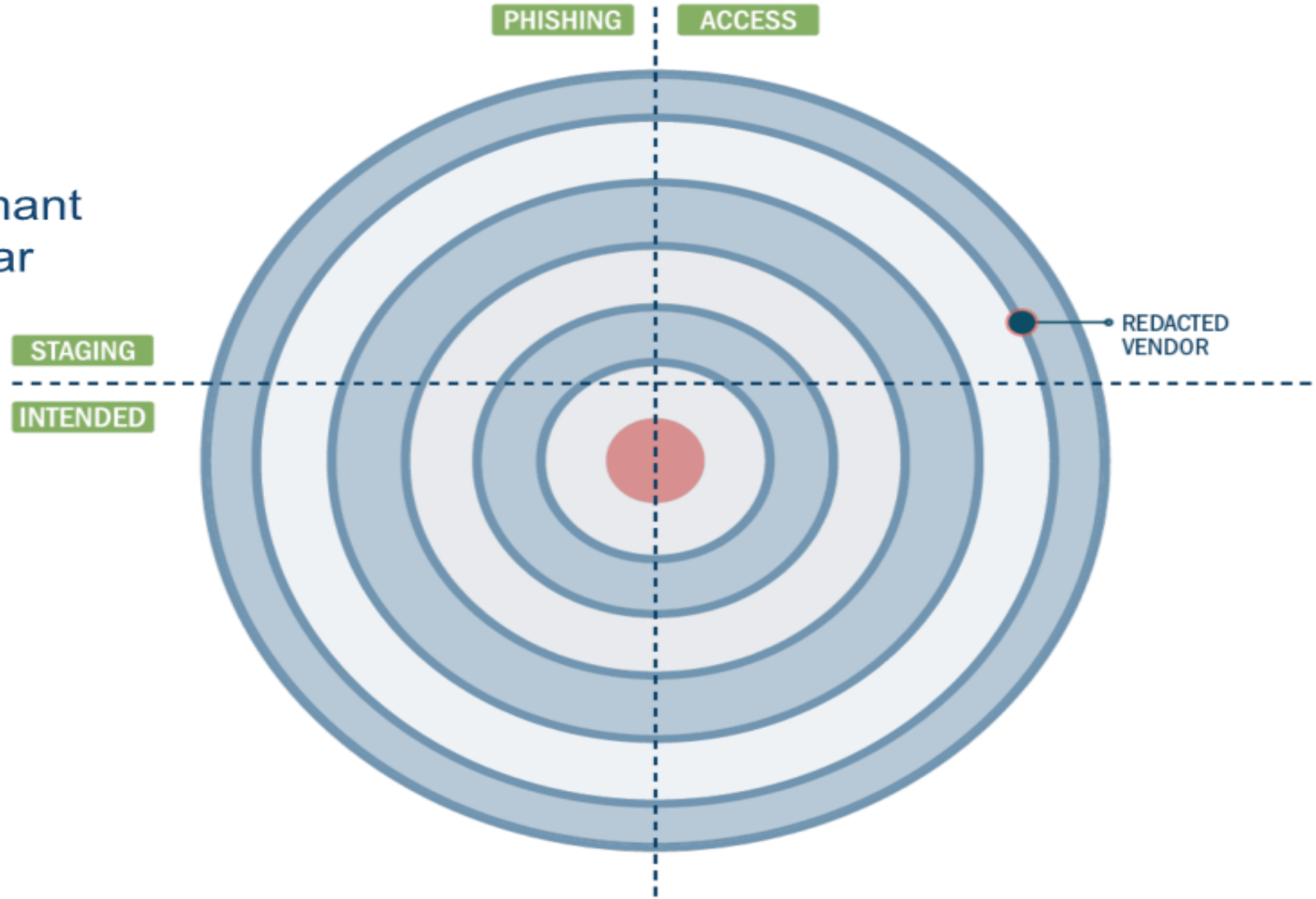


- **Advanced Persistent Threat** (APT) actors
- **Hundreds of victims** (targeted or affected)
  - Energy (focus area)
  - Nuclear
  - Aviation
  - Critical manufacturing
  - Government entities
- **Response effort** coordinated between multiple government organizations as well as industry organizations
- **Effect has been limited to access** so far, with no physical impact identified

TLP:WHITE

# Campaign Timeline

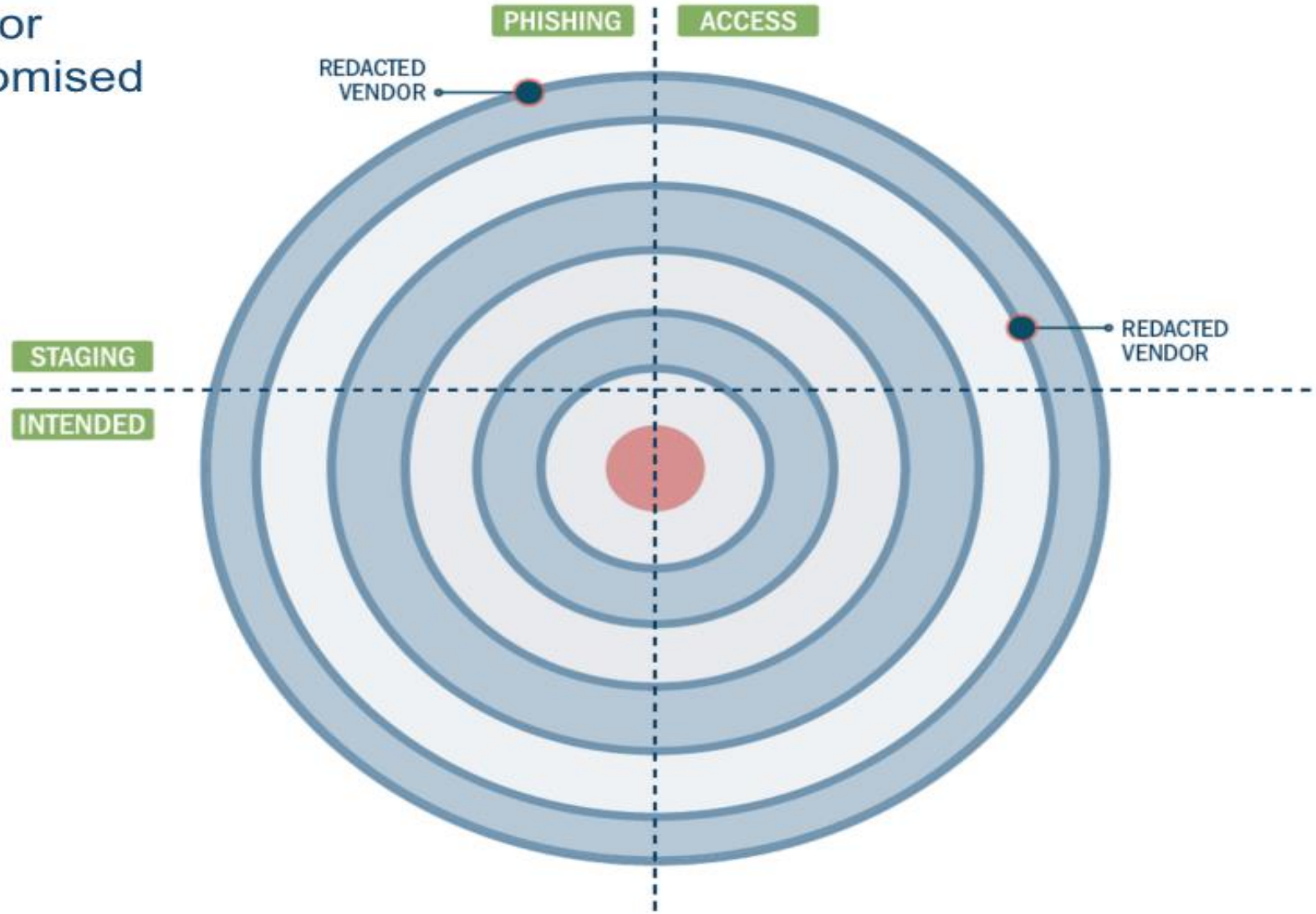
- Vendor compromised in early 2016
- Remained dormant for over one year



TLP:WHITE

# Campaign Timeline

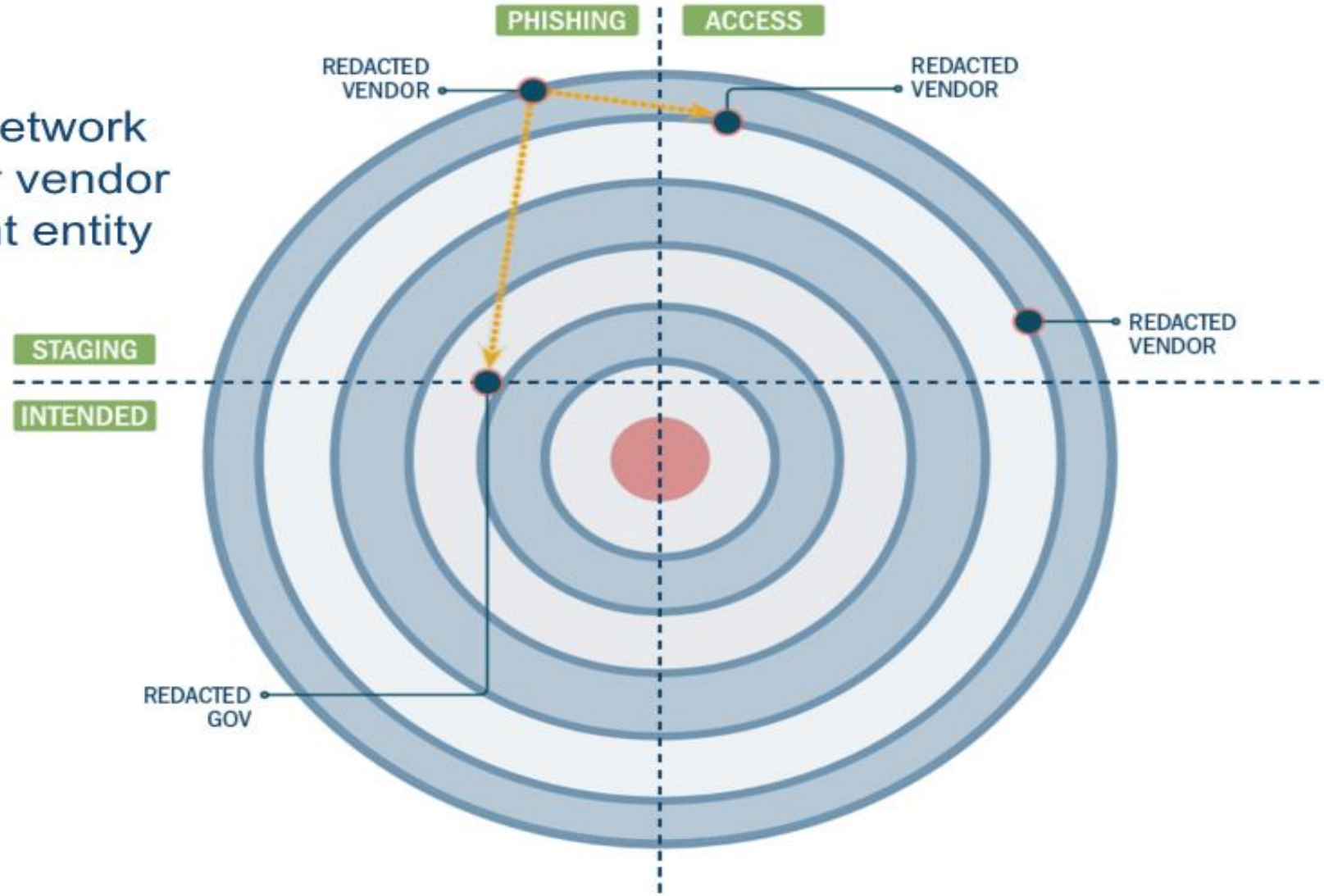
- Additional vendor network compromised in early 2017



TLP:WHITE

# Campaign Timeline

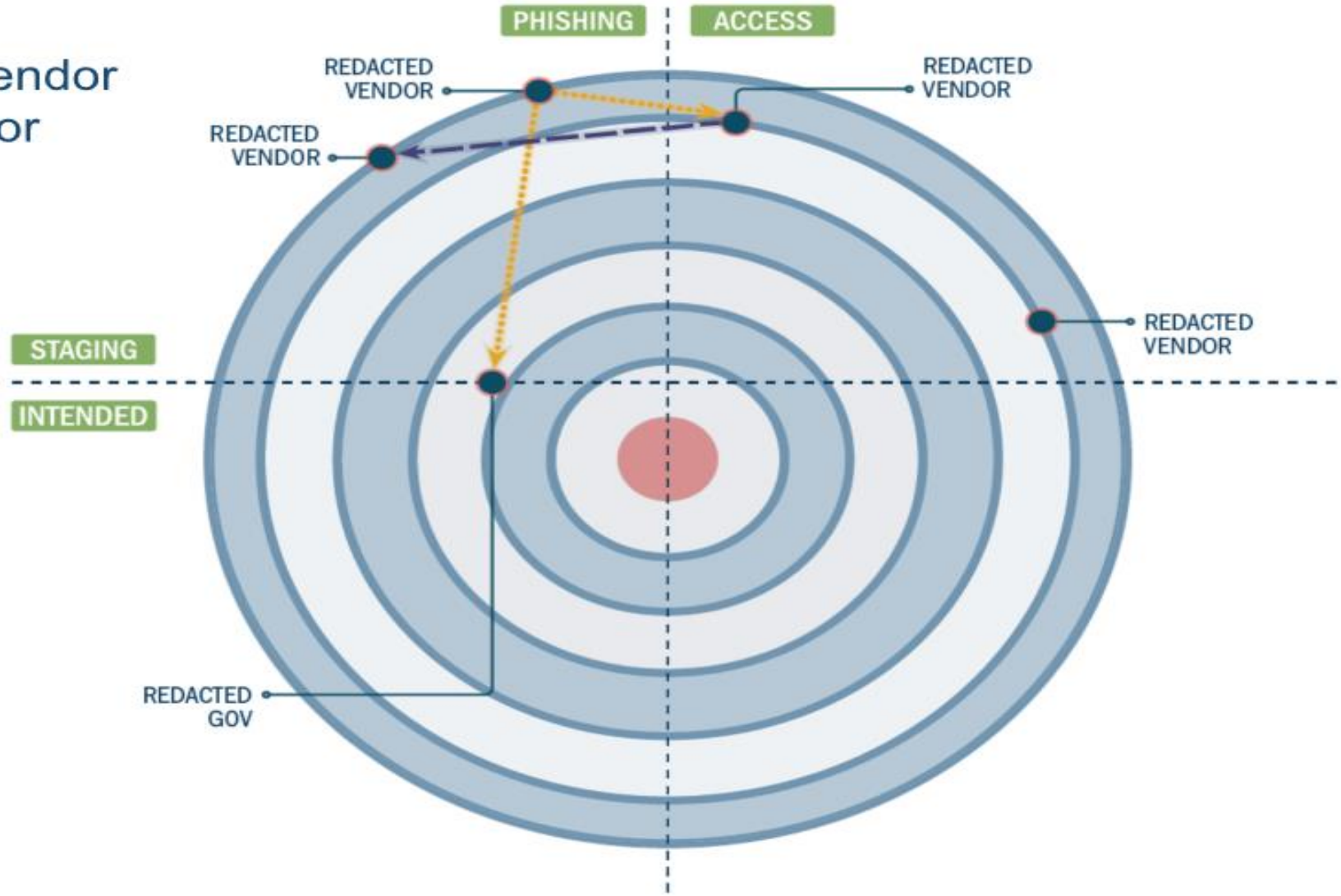
- Phishing attack originating from compromised network against another vendor and government entity



TLP:WHITE

# Campaign Timeline

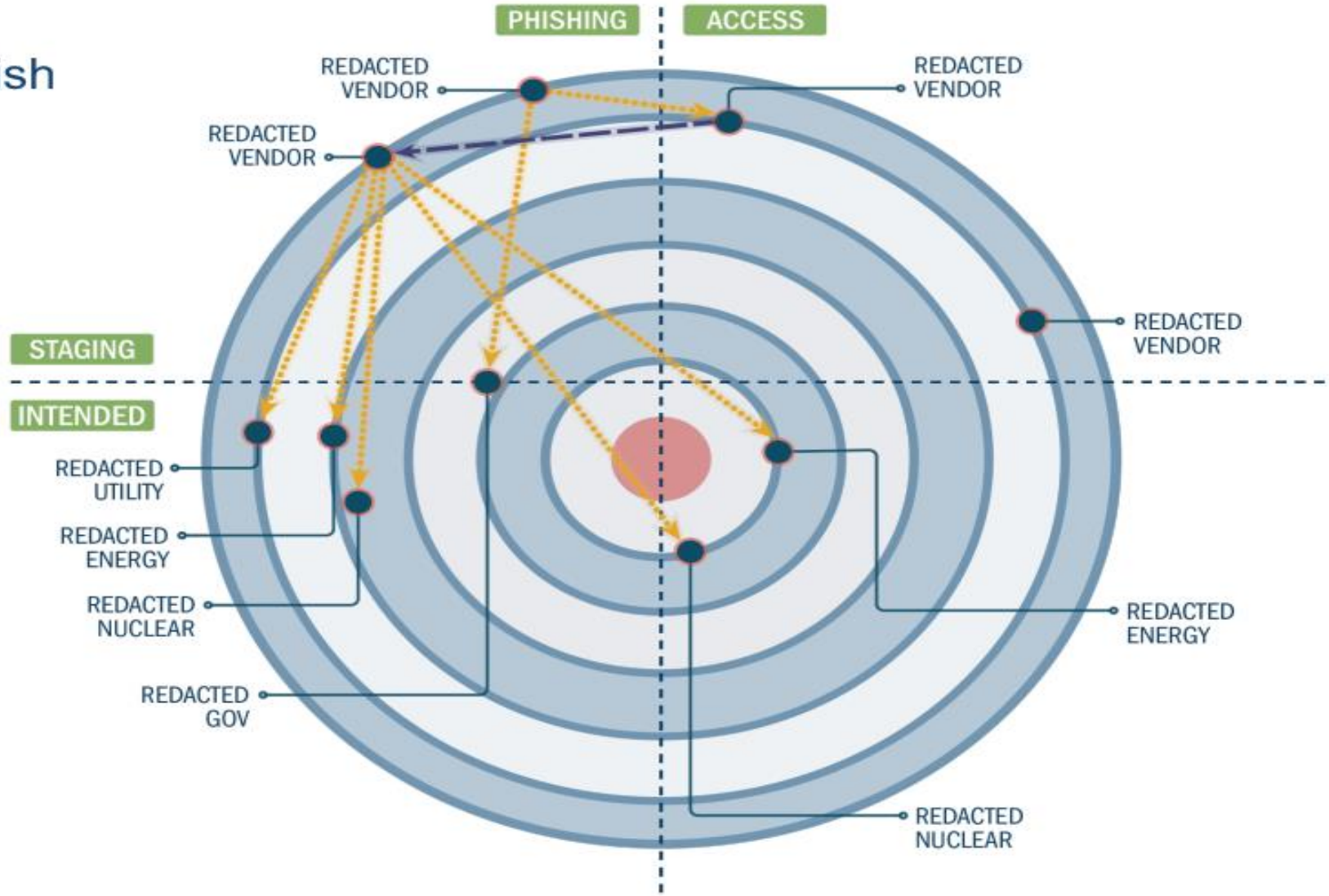
- Intrusion from compromised vendor to another vendor



TLP:WHITE

# Campaign Timeline

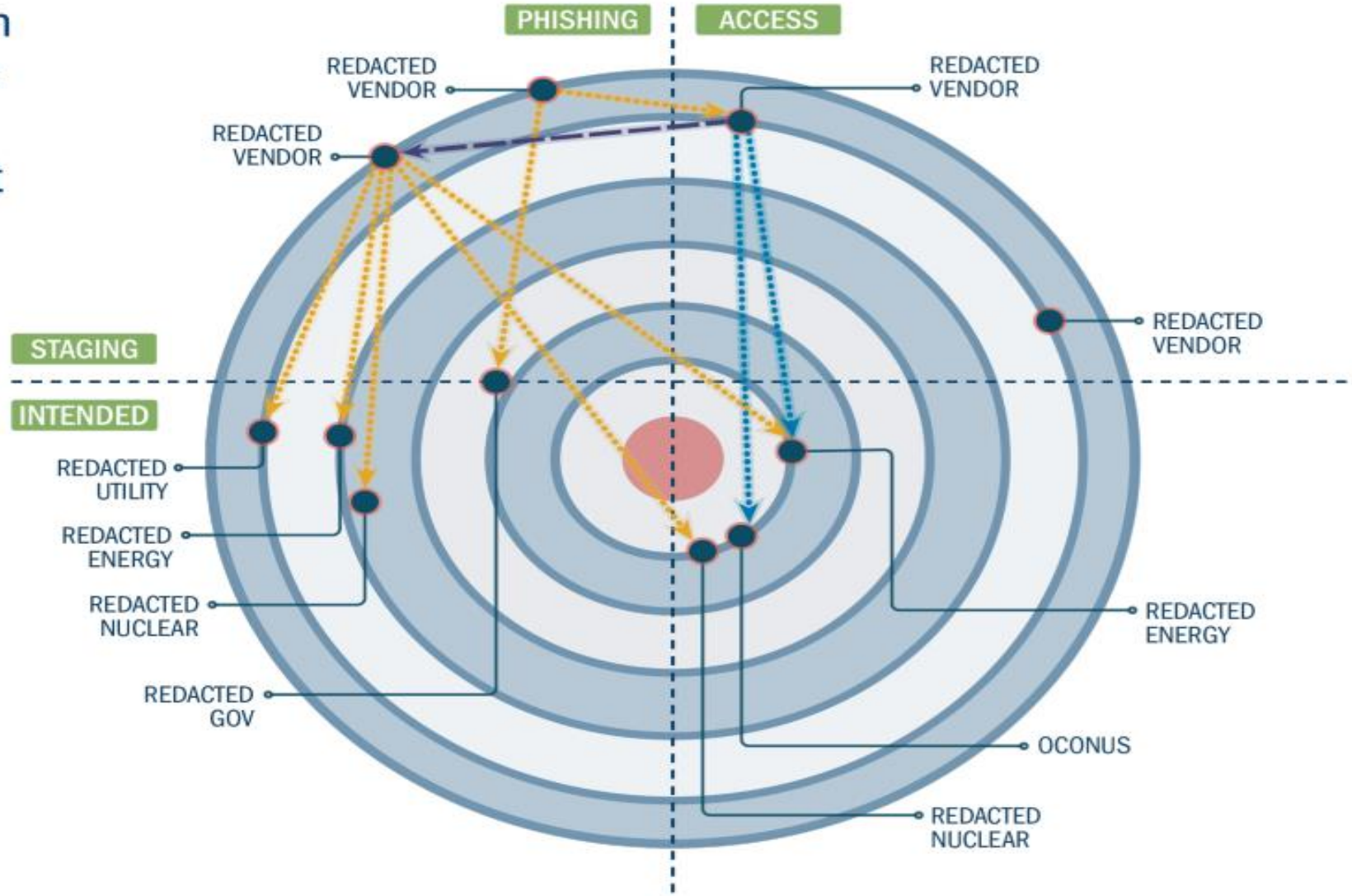
- Vendor victim leveraged to phish U.S. utilities



TLP:WHITE

# Campaign Timeline

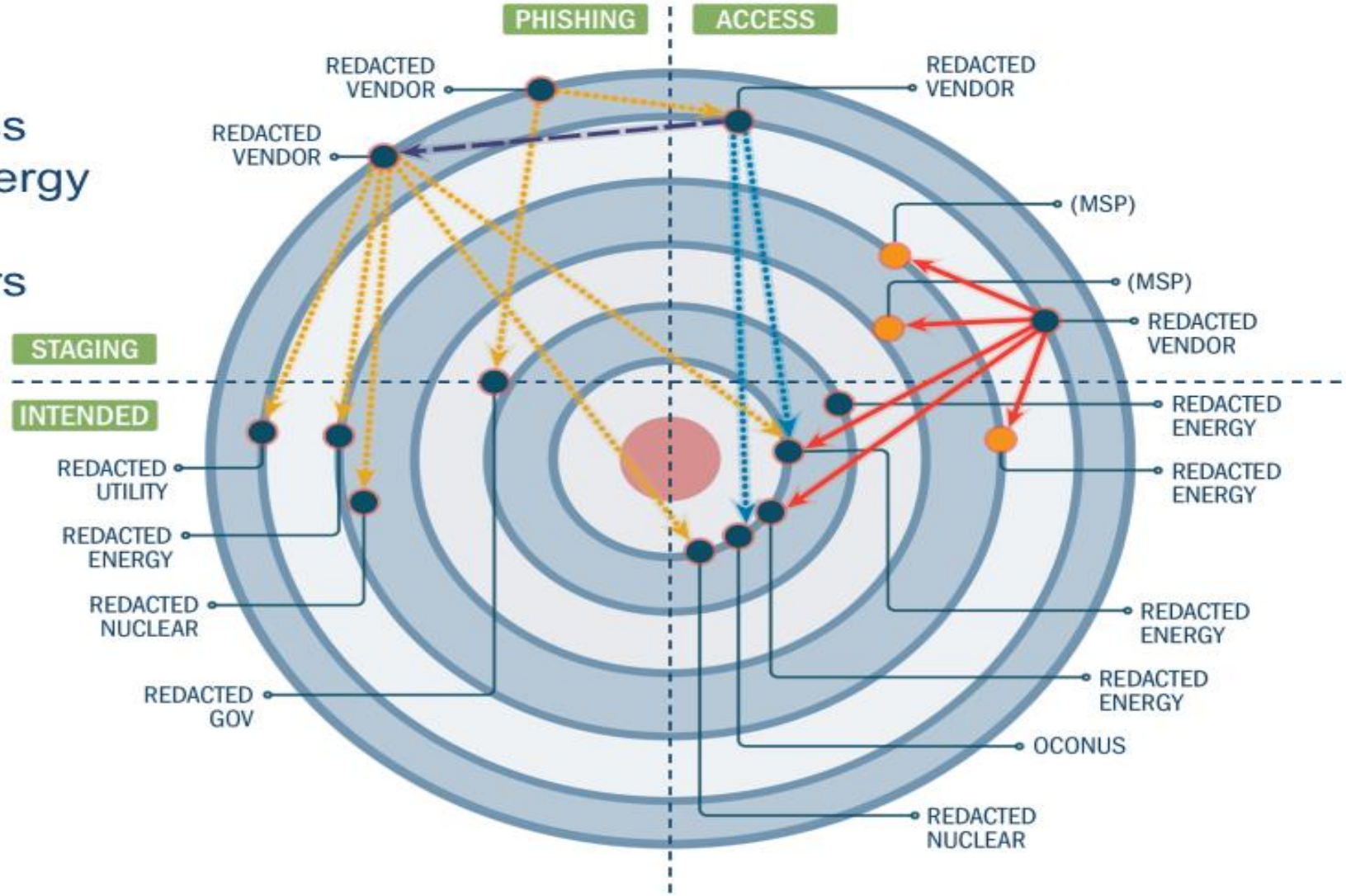
- Used new victim network to pivot and browse external content of an already-phished organization, as well as a non-U.S. organization



TLP:WHITE

# Campaign Timeline

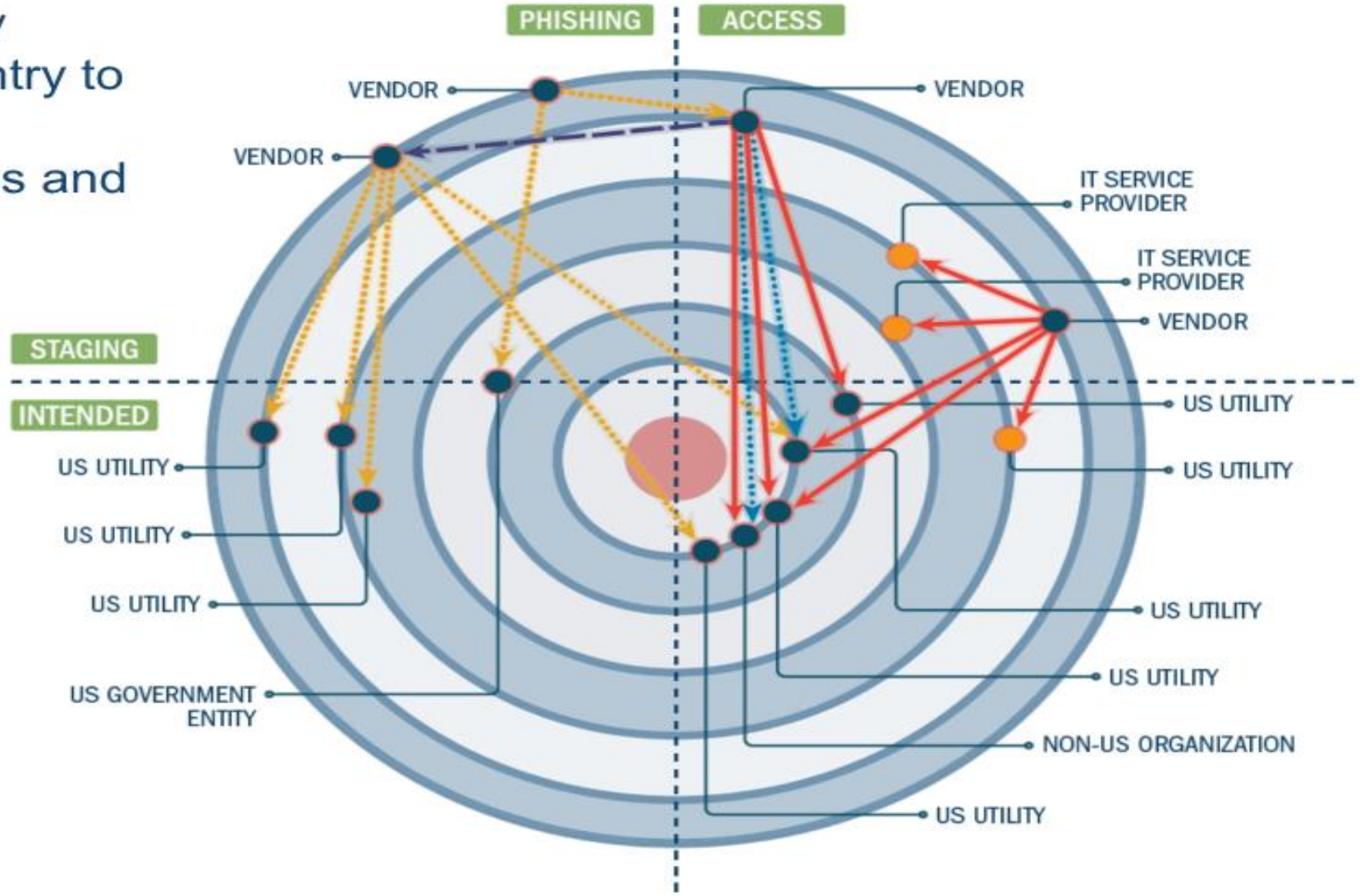
- Used initial compromised vendor to access several U.S. energy utilities and IT service providers



TLP:WHITE

# Campaign Timeline

- Leveraged early victim to gain entry to two previously accessed utilities and one new victim



TLP:WHITE

# Who is the Target?

**Staging Targets**

- **Smaller organizations** with less sophisticated networks
- **Pre-existing relationships** with intended targets
- **Deliberately selected**, not targets of opportunity
- Examples: **vendors, integrators, suppliers,** and **strategic R&D partners**
- Used for **staging tools** and **capabilities**

**Intended Targets**

- **Small, medium,** and **large organizations**
- U.S. targets focused within the **Energy Sector**, specifically power generation, transmission, and distribution
- **Sophisticated networks** with more defensive cyber tools

POLITICS

# Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Blackouts could have been caused after the networks of trusted vendors were easily penetrated

Hackers working for Russia claimed "hundreds of victims" last year in a giant and long-running campaign that put them inside the control rooms of U.S. electric utilities where they could have caused blackouts, federal officials said. They said the campaign likely is continuing.

"They got to the point where they could have thrown switches" and disrupted power flows, said Jonathan Homer, chief of industrial-control-system analysis for DHS.

Officials of the Department of Homeland Security said hackers have reached the control rooms of U.S. electric utilities. **PHOTO:** ANDREW HARRER/BLOOMBERG NEWS

*By Rebecca Smith*

July 23, 2018 7:21 p.m. ET

# Russian Activity Update

- Of the 100 “phished”, approximately 20 were hooked
- 12 of the 20 accounted for 45% of electricity delivered in the US
- NPPD does not appear to be one of the “chosen ones”

# Supply Chain Threat

# Threats…..


Source : *Software Assurance Forum October 2008*

# Triton/TRISIS/"Hatman" Malware

- Affects Triconex Tricon safety controllers
- Supply Chain attack example
- NPPD does have impacted equipment at SS1, GGS, and CNS


Tricon Tricon CX
EcoStruxure Triconex Safety Systems

# Business Email Compromise (BEC)

Nebraska Public Power District

*Always there when you need us*

# An Example of BEC

From: Vincent, Craig A.- York [mailto:cavince@nppd.com]
Sent: Friday, October 12, 2018 9:58 AM
To: Cindy Cruse
Subject: November 2 Annual Auction

Hi Cindy! Can you tell me the ticket prices for the November 2 event and whether you're offering corporate tables?

Craig A. Vincent

Nebraska Public Power District

Account Manager

402-362-7305

402-366-7209

# An Example of BEC

From: Cindy Cruse <ccruse@plattsmouthchamber.com>

Date: Friday, Oct 12, 2018, 10:22 AM

To: Vincent, Craig A.- York <cavince@nppd.com>

Subject: RE: November 2 Annual Auction

This email is from ccruse@plattsmouthchamber.com. Do you know them and are you expecting this? - Look again!
Use the "Report Phishing" button if you think this is a phishing email.
Phishing is the #1 threat to NPPD. You are our best defense!!
Stay Vigilant!

---

They are $75 a ticket or $600 for a corporate table of 8 J

# An Example of BEC

From: Vincent, Craig A.- York
Sent: Friday, October 12, 2018 7:43 PM
To: Cindy Cruse
Subject: RE: November 2 Annual Auction

Please reserve a table for NPPD.

Sent with BlackBerry Work
(www.blackberry)

Craig Vincent
Account Manager
Nebraska Public Power District
402-366-7209

From: Cindy Cruse <ccrusse@planetmail.com>
Date: Monday, Oct 22, 2018, 12:02 PM
To: Vincent, Craig A.- York <cavince@nppd.com>
Subject: RE: November 2 Annual Auction

This email is from ccrusse@planetmail.com. Do you know them and are you expecting this? - Look again!
Use the "Report Phishing" button if you think this is a phishing email.
Phishing is the #1 threat to NPPD. You are our best defense!!
Stay Vigilant!

---

Craig, i would like you to send it as bank transfer or by money gram or western union, kindly let me know so i can info that i need to send you..

I aplogize for the sudden notification,kindly bear with me.

On Mon, Oct 22, 2018 at 9:22 AM Vincent, Craig A.- York wrote:

Hi Cindy,

I received your invoice for the Chamber event. I'd like to pay by credit card. Let me know when you're in the office and available to take care of this.

Craig

**From:** Cindy Cruse <ccrusse@planetmail.com>
**Sent:** Monday, October 22, 2018 3:36 PM
**To:** Vincent, Craig A.- York <cavince@nppd.com>
**Subject:** Re: RE: November 2 Annual Auction

This email is from ccrusse@planetmail.com. Do you know them and are you expecting this? - Look again!
Use the "Report Phishing" button if you think this is a phishing email.
Phishing is the #1 threat to NPPD. You are our best defense!!
Stay Vigilant!

---

Thanks for you email, this is what you can do now,buy an Itune gift card or Amazon gift card take picture of it and send and we can take it that way..

I appreciate your co-operation.

> **Sent:** Monday, October 22, 2018 at 10:21 AM
> **From:** "Vincent, Craig A.- York"
> **To:** "Cindy Cruse"
> **Subject:** RE: November 2 Annual Auction
>
> How about if I send it through accounts payable and they cut a check?
>
> Sent with BlackBerry Work
> (www.blackberry)

# What Can We Do?

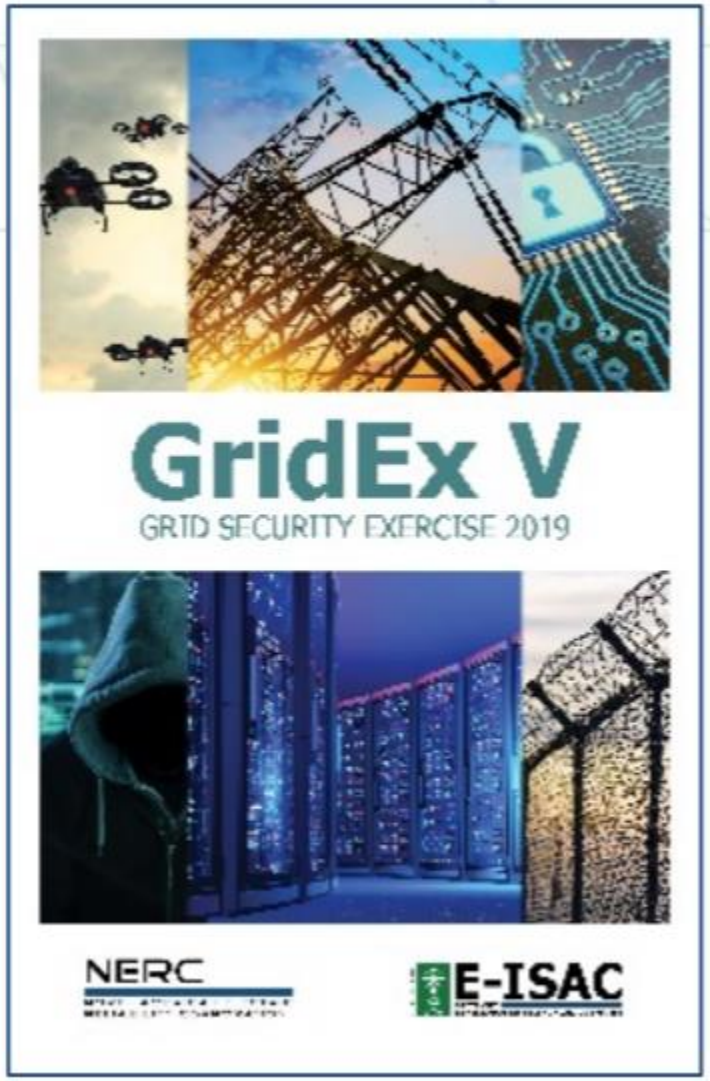
# Three (3) Things that can help

1. Have a Recovery Plan…and practice it!
2. Have multiple layers of defense…and email protection is a must!
3. Keep Security in your employees “Front of Mind”…using whatever means possible!!

# Have a Recovery Plan..and practice it!

The objectives for GridEx V are:

- Exercise incident response plans
- Expand local and regional response
- Engage interdependent sectors
- Increase supply chain participation
- Improve communication
- Gather lessons learned
- Engage senior leadership



# Have multiple layers of defense…and email protection is a must!

# Keep Security in your employees “Front of Mind”…using whatever means possible!!

Nebraska Public Power District

*Always there when you need us*

STOP | THINK | CONNECT™

Visit ***www.dhs.gov/stopthinkconnect*** for more information on how to get involved with the Stop.Think.Connect. Campaign.

**SECURING ONE CITIZEN, ONE FAMILY, ONE NATION AGAINST CYBER THREATS.**

# STOP. THINK. CONNECT.™

Protect yourself and help keep the web a safer place for everyone.

# INSECURE

## AN NPPD SHORT FILM

# Three Takeaways…

- Threats against Critical Infrastructure are real and increasing.
- Your employees are your biggest weakness and your best ally.
- Be prepared by having a plan and keeping your employees on-guard.

# Questions?