

RUSS HORN

Cybersecurity 101



1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.

Opinions may not reflect the opinions of AccountingWare.

This presentation is proprietary.

Unauthorized release of this information is prohibited.
Original material is copyright © 2023 AccountingWare.



2

Agenda

HERE'S THE PLAN

- Introduction
- Cyber Attack Story
- Cybersecurity Hot Topics
- Security Best Practices
- ActivityHD ActivWebAPI, Self-Serve, & Aspire Hosting



3



Russ Horn

PRESIDENT

CISA, CISSP, CRISC



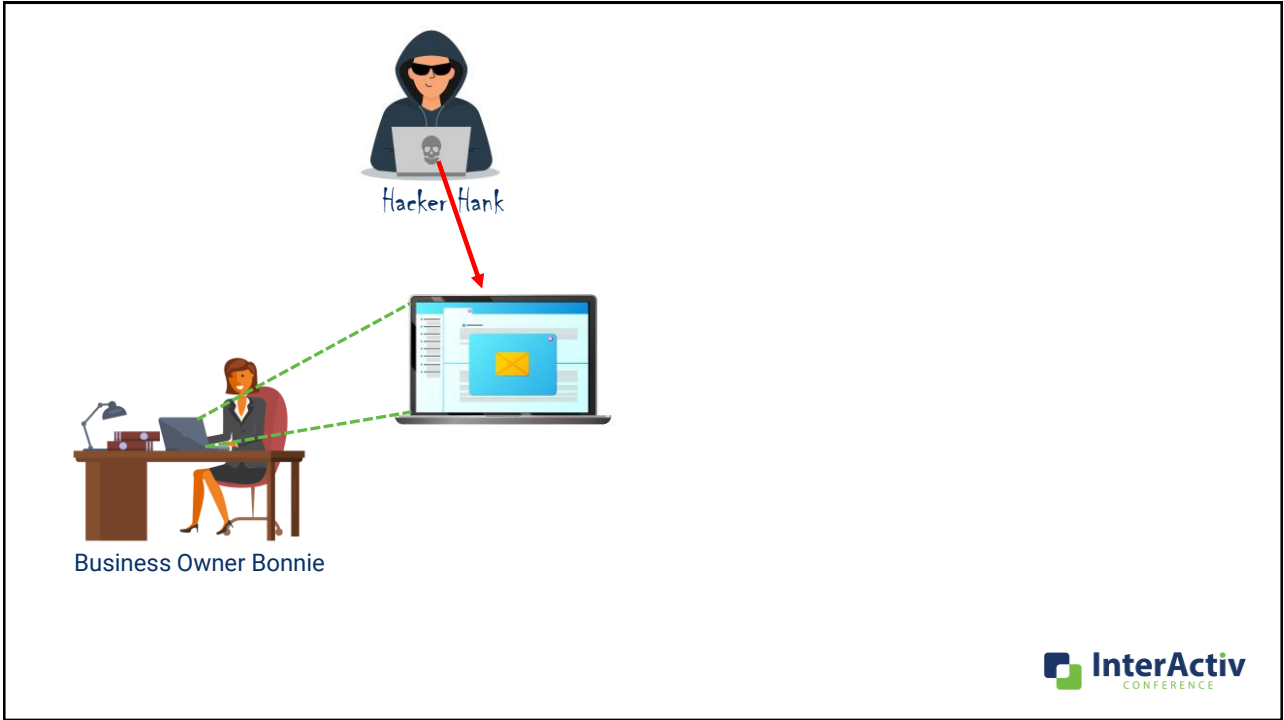
4

The diagram features the CoNetrix logo at the top center, which consists of a red circular icon with two arrows forming a loop, followed by the text "CoNetrix" in a bold, dark blue font. Below this, the tagline "A Family of Technology Companies" is written in a smaller, dark blue font. A horizontal line runs across the middle of the slide, with four circular icons placed on it. From left to right, these icons are: 1) AccountingWare, with a green and blue "AW" logo and the text "AccountingWare." below it; 2) CoNetrix Technology, with a green circular icon and the text "CoNetrix Technology" below it; 3) CoNetrix Security, with a blue circular icon and the text "CoNetrix Security" below it; and 4) Tandem, with a red and blue diamond-shaped icon and the text "Tandem" below it. In the bottom right corner of the slide, the InterActiv CONFERENCE logo is displayed, featuring a blue and green square icon and the text "InterActiv CONFERENCE".

5

This slide has a light gray background. In the top right corner, the InterActiv CONFERENCE logo is present. The main content of the slide is the title "Cyber Attack Story" in a large, bold, dark blue font. Below the title, the phrase "BASED ON A TRUE STORY" is written in a smaller, green, all-caps font. A white curved line starts from the bottom left and curves upwards towards the center of the slide.

6



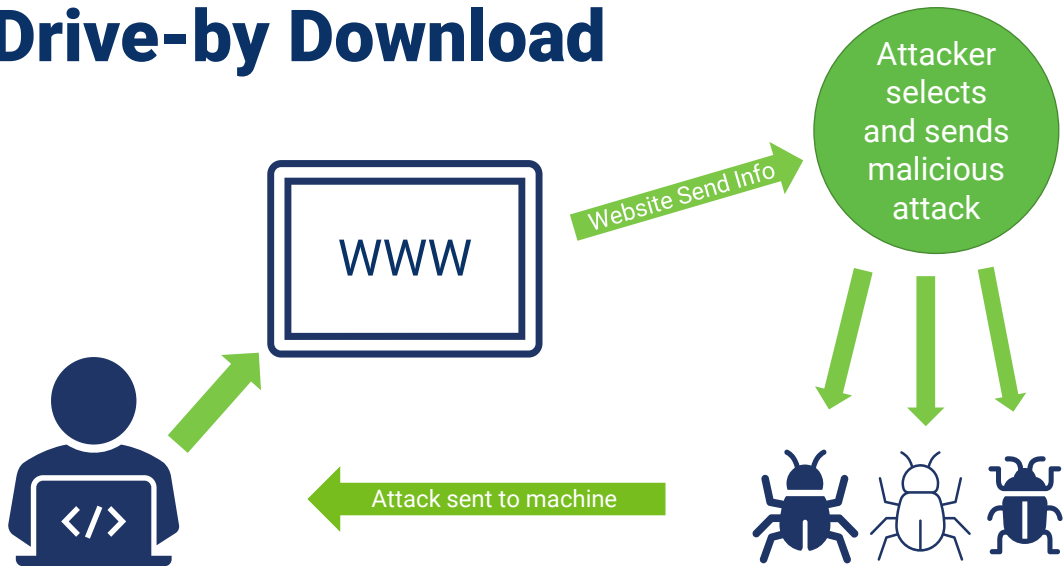
7

3 Possible Attacks

1. Drive-by Download Attack
- 2.
- 3.

8

Drive-by Download



9

3 Possible Attacks

1. Drive-by Download Attack
2. Compromised Password

10

Compromised Password



Gussed Password



Keylogger



Pulled from Known Passwords



11

Password Tips

SAMPLE SUBTITLE

1

Don't use the same password.

2

Consider longer passwords.

3

Consider a password vault.

4

Change your password.

5

Use Multi-Factor Authentication.



12

Multi-Factor Authentication



13

3 Possible Attacks

1. Drive-by Download Attack
2. Compromised Password
3. Phishing Attack

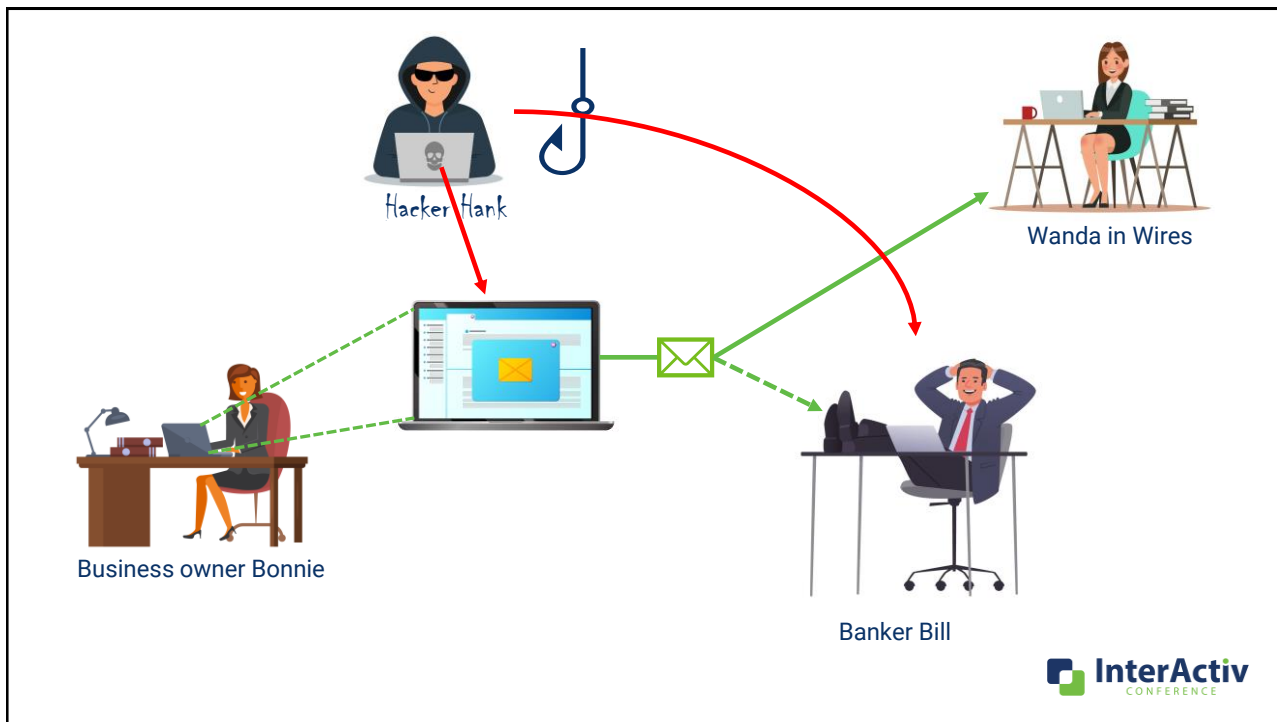
14

Phishing Attack



WHALING

A specific type of phishing that targets the senior executives of an organization.



17

Phishing Attack

File Message Adobe PDF Tell me w...

Voice message notification f...

ES0 Synantec VIP

https://dskd1.com/voices/webnet.php?code=2018900

Outlook

me@you.com

Verify your email Password to Proceed

Confirm Your Identity

For your protection confirm your email address.

Email Address

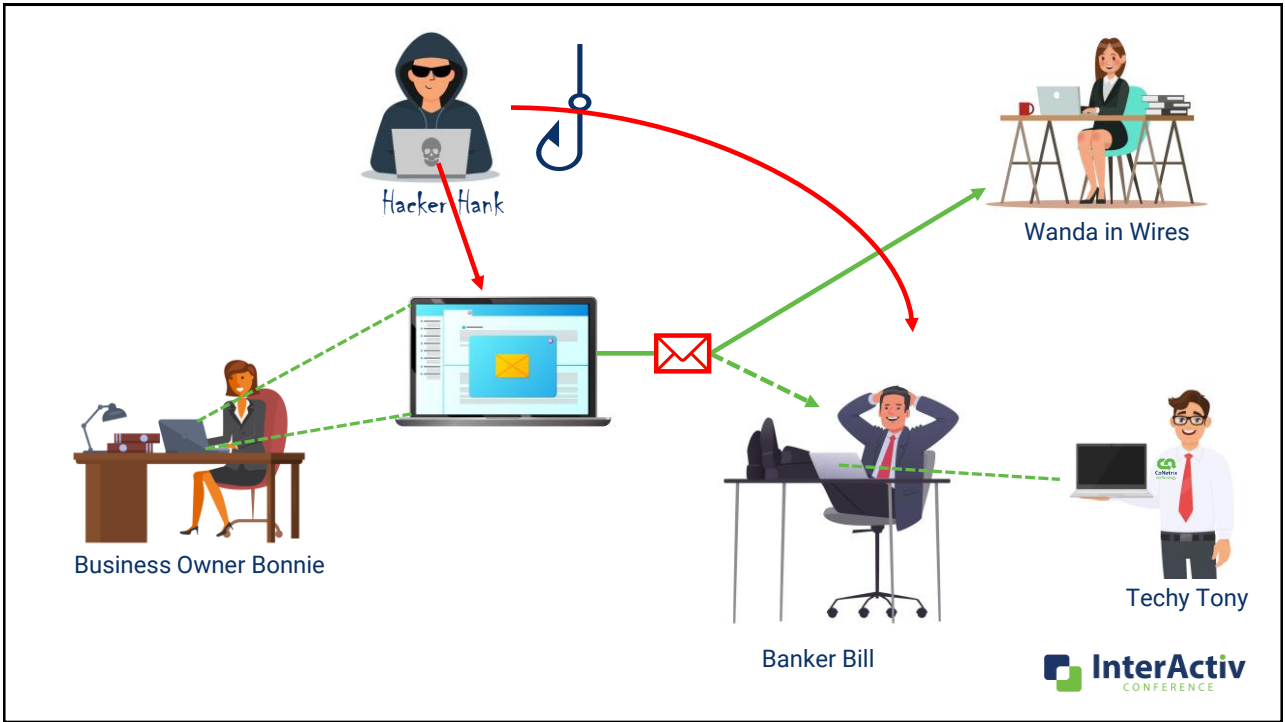
Remember this device

Cancel Continue

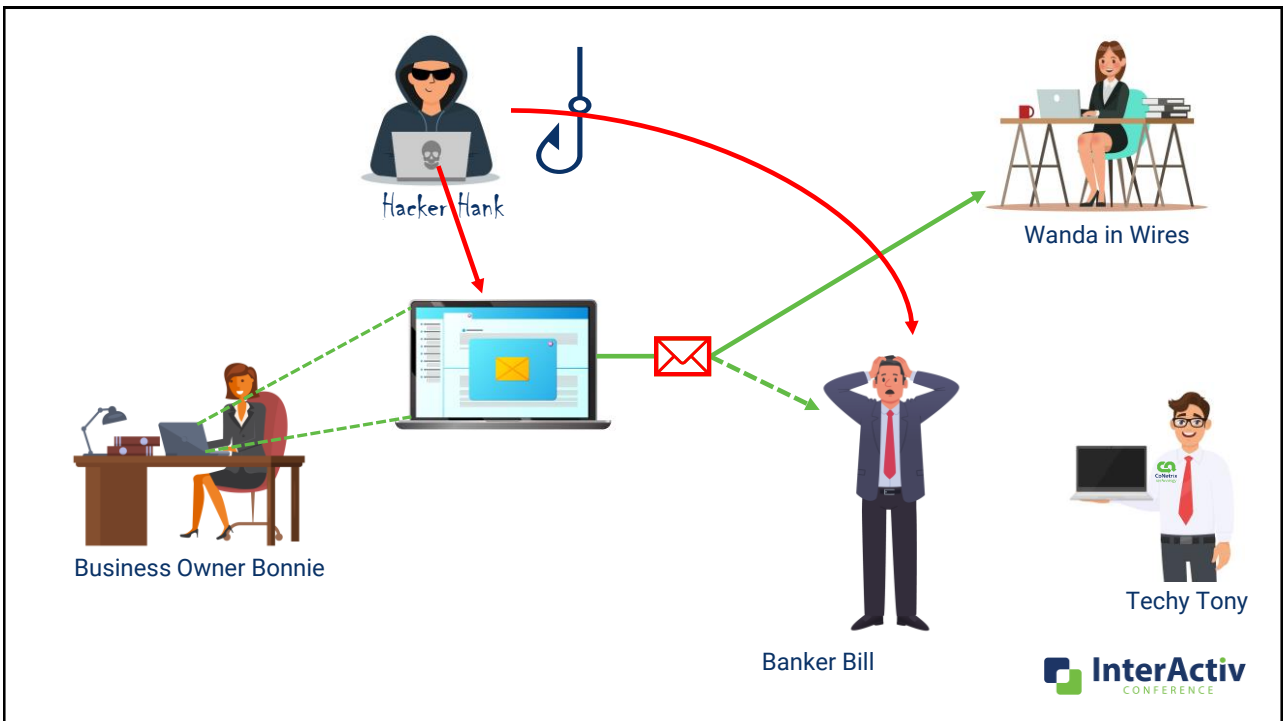
Cancel download 192kb

InterActiv CONFERENCE

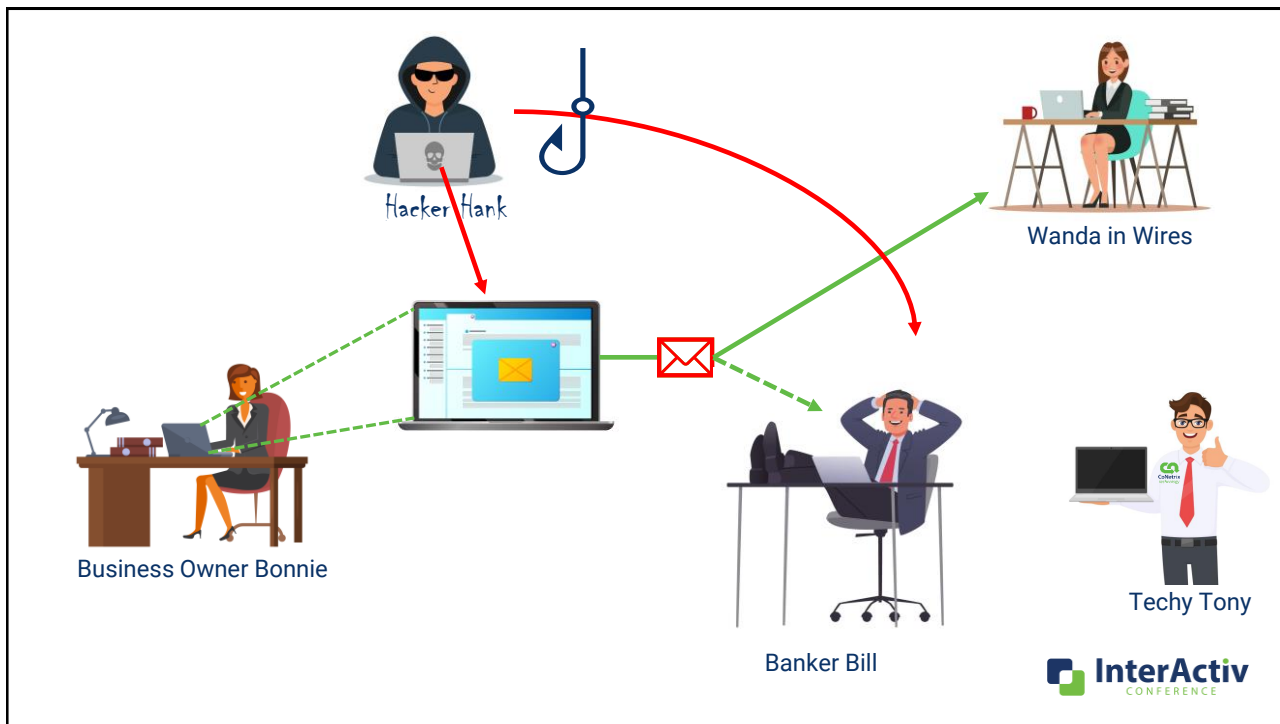
18



19



20



21

InterActiv CONFERENCE

Cybersecurity Hot Topics

22



23

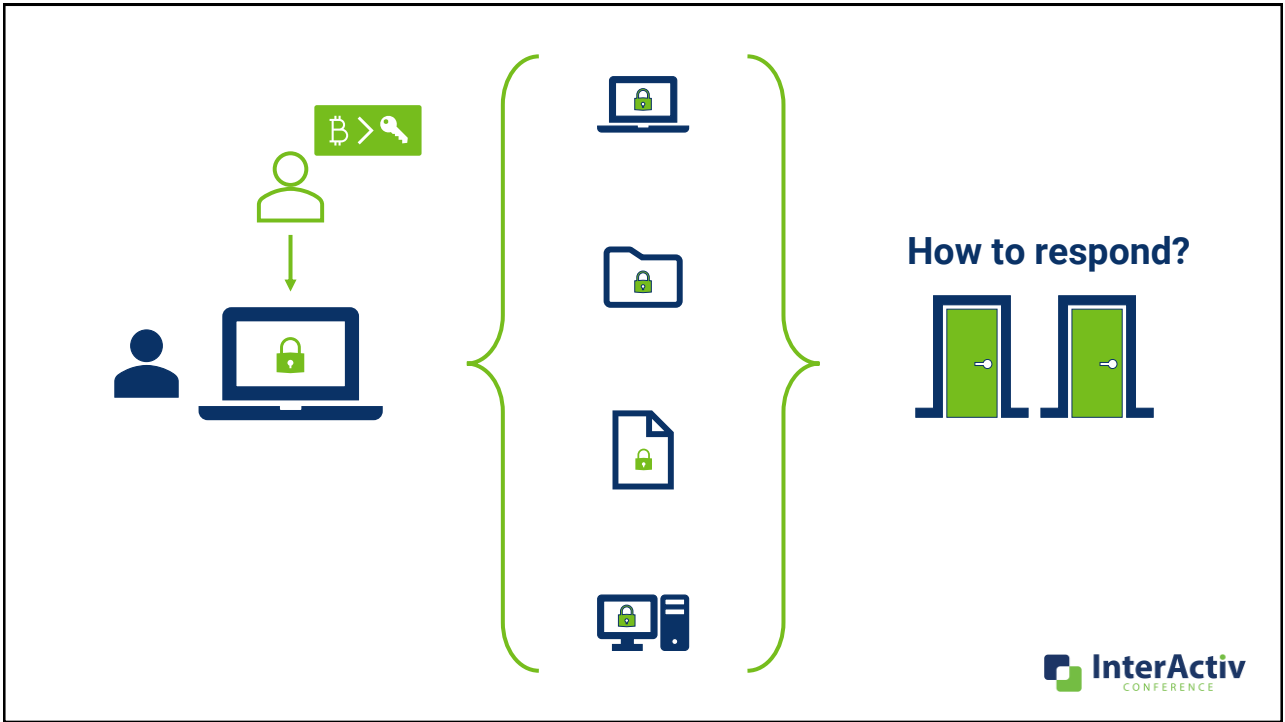
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

“Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.”

<https://us-cert.cisa.gov/ncas/tips/ST19-001>

InterActiv
CONFERENCE

24



25



26

If we pay the ransom:



High Cost



Complex Payments



No Guarantees



Bigger Target



Supports Business Model



Legal Consequences



27

If we rebuild the system:



Invest Time and Money



Rebuild All Affected Systems



Restore Clean Data Backups



28

Questions to Ask

- What protections do we have in place?
- Are all critical systems backed up?
- How would we recover from our backups?
- Have we conducted ransomware specific table-top tests?



Ransomware

29

RESOURCE

Case Study: Small Business Survives an Active Ransomware Attack

CoNetrix.com/Ransomware



CoNetrixTechnology CUSTOMER CASE STUDY

CASE STUDY
Small Business Survives an Active Ransomware Attack

Ransomware continues to be a challenge for organizations of all sizes around the world. Unfortunately, the trend from the past few years is that ransomware and business email compromise attacks are on the increase. Here are some sobering statistics:

- A new organization falls victim to ransomware every 14 seconds in 2018 and is estimated it will be every 11 seconds in 2021. (CyberSecurity Ventures)
- Phishing emails are the vector for two-thirds of ransomware infections. (Status)
- 40% of ransomware operators impersonate authority figures such as the FBI or the IRS. (Stanford University)
- aCrime, defined as criminal activities in order to generate revenue, have increased to 70% of all operations between 2018 and 2020. (CrowdStrike 2021 Global Threat Report)

As a Managed Service Provider (MSP), CoNetrix Technology has helped many customers secure their IT infrastructure against ransomware and successfully responded to ransomware attacks to stop or limit the damage. The purpose of this case study is to describe a specific ransomware attack against one of our customers and how the attack was successfully thwarted. The goal is to provide information to other organizations so they can learn from this specific attack and better protect their IT environment.

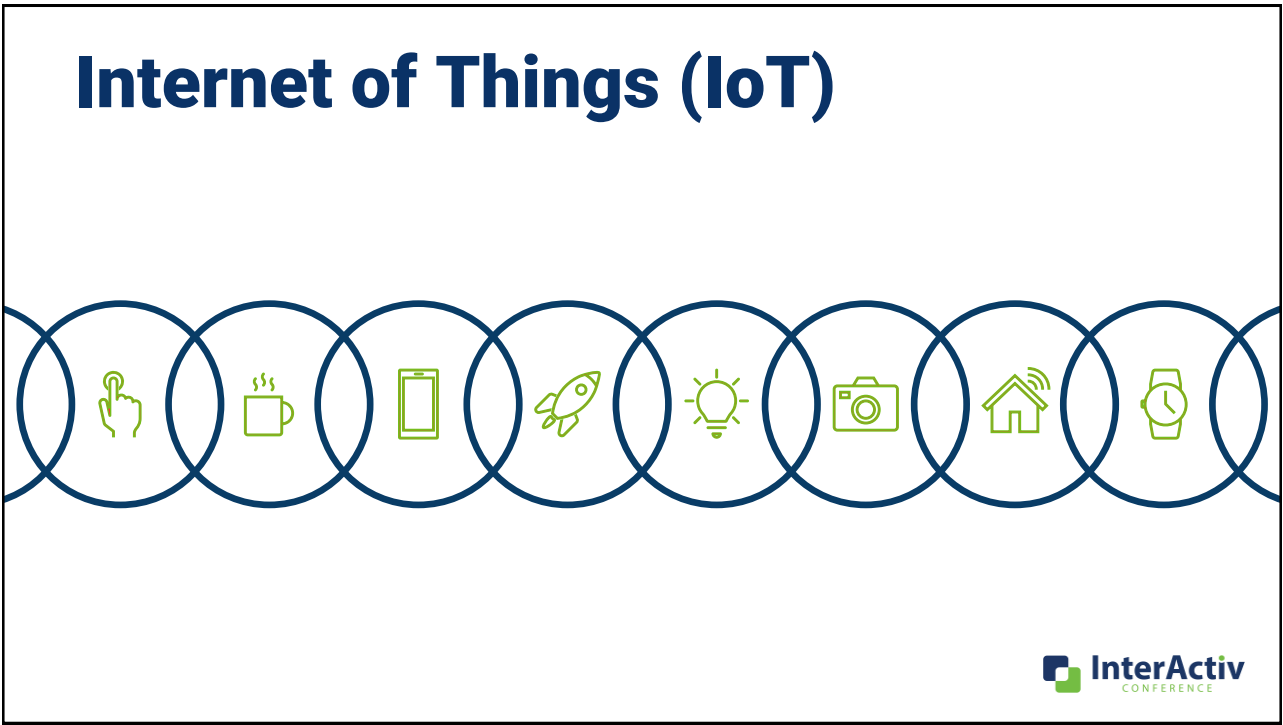
INCLUDES
Every IT environment is slightly different, so strategies described in this case study may not apply to your situation.
Similarly, every attack is different, and the attack vectors are constantly changing. So over time the responses we describe in this case study may not apply to future attacks.
We are not disclosing any customer-specific information to protect their confidentiality and prevent making them a target for future attacks.

BACKGROUND AND CONTEXT: customer's IT environment: Windows 10 virtual desktops available through Citrix Cloud and a hosted Citrix Remote Access Gateway. Windows servers running on VMware vSphere. Endpoint protection provided through CoNetrix Technology, based on CyberoProtect and CylanceOptics.
Email backed with a different service provider using basic email filtering. FortiGate Unified Threat Management appliance installed on the customer premise and managed by CoNetrix.

30



31



32



Internet of Things

Questions to Ask

- Do we allow IoT on our company network?
- How do we patch IoT devices?



33

Techy Tony



Security Best Practices

34

Security Best Practices



Install patches



Anti-malware software



Strong passwords (MFA where possible)



Don't run as a local administrator



Be cautious of phishing attempts



35



ActivityHD Security Controls

36



37

ActivWebAPI

- Two ways to use ActivWebAPI:
 - Self-Serve
 - Automation
- Security:
 - Encryption
 - Multi-Factor Authentication (MFA)

38



39

Self-Serve

- Access via a web portal over the Internet or corporate intranet
- Self-Serve currently supports:
 - Payroll
 - Purchasing
 - Accounts Payable
- Security:
 - Encryption
 - Multi-Factor Authentication (MFA)

40

Aspire Hosting



41

Aspire Hosting

ACTIVITYHD HOSTED BY ASPIRE

- Advantages of Cloud Hosting with Aspire
 - Managed technology & security
 - Patch management, ActivityHD, and security updates
 - Scheduled data backups and disaster recovery
 - SOC 1 Type 2 reviewed datacenter



42



InterActiv
CONFERENCE

THANKS FOR JOINING!

Cybersecurity 101

Russ Horn
CISA, CISSP, CRISC

The slide features a decorative background with a light gray floral pattern on the left side, transitioning into a white background on the right. The InterActiv logo is positioned in the top left corner. The main title 'Cybersecurity 101' is prominently displayed in the center-right, with the speaker's name and credentials below it.