/whois

Brett L Scott - Director level at TD SYNNEX

Cybersecurity professional - hacker - urban farmer

Programmer since 1987 (professionally)

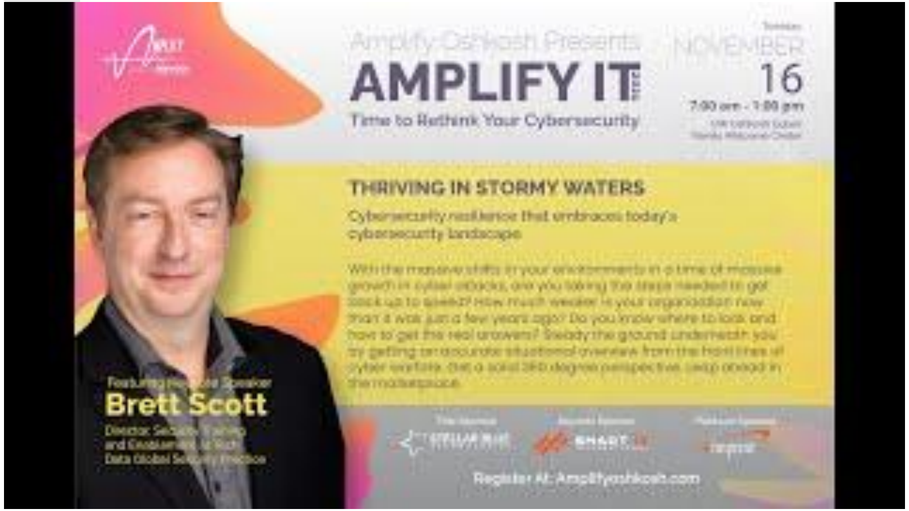
Hands-on technical

Founder the National Cyber War Foundation and

The Arizona Cyber Warfare Range

The Wisconsin Cyber Threat Response Alliance, Michigan, Georgia, Wyoming

2021 Amplify Oshkosh



Amplify Oshkosh Presents

AMPLIFY IT 2021

Time to Rethink Your Cybersecurity

Tuesday
NOVEMBER
16
7:00 am - 1:00 pm
UW Oshkosh Culver
Family Welcome Center

THRIVING IN STORMY WATERS

Cybersecurity resilience that embraces today's cybersecurity landscape

With the massive shifts in your environments in a time of massive growth in cyber attacks, are you taking the steps needed to get back up to speed? How much weaker is your organization now than it was just a few years ago? Do you know where to look and how to get the real answers? Steady the ground underneath you by getting an accurate situational overview from the front lines of cyber warfare. Get a solid 360 degree perspective. Leap ahead in the marketplace.

Featuring Keynote Speaker
Brett Scott
Director, Security Training and Enablement, NTT Data Global Security Practice

Title Sponsor — Keynote Sponsor — Platinum Sponsor

Register At: Amplifyoshkosh.com

https://www.youtube.com/watch?v=B-IBmRfL5rw&t=750s

I have a face for radio

What do you think?

Which speech was better?

What medium is better?

What medium is more effective?

The audio clip was a deep fake!

Cybersecurity and Regulatory Constructs

The Finance executives speak…

- During the past 12 months, 34.5% of polled executives report that their organizations' accounting and financial data were targeted by cyber adversaries.
- Within that group, 22% experienced at least one such cyber event and 12.5% experienced more than one.
- Nearly half (48.8%) of C-suite and other executives expect the number and size of cyber events targeting their organizations' accounting and financial data to increase in the year ahead.

- Just 20.3% of those polled say their organizations' accounting and finance teams work closely and consistently with their peers in cybersecurity.
- **Nearly half of executives expect cyber-attacks targeting accounting, other systems**

Source: Deloitte Center for Controllership poll

The losses are significant

In 2022, 76% of organizations were targeted by a **ransomware** attack, out of which 64% were actually infected. Only 50% of these organizations managed to retrieve their data after paying the ransom. Additionally, a little over 66% of respondents reported to have had multiple, isolated infections.

A research company Trellix determined 78% of business email compromise (BEC) involved fake CEO emails using common CEO phrases, resulting in a 64% increase from Q3 to Q4 2022. Tactics included asking employees to confirm their direct phone number to execute a voice-phishing – or vishing – scheme. 82% were sent using free email services, meaning threat actors need no special infrastructure to execute their campaigns

Federal Trade Commission (FTC) data shows that consumers reported losing nearly $8.8 billion to fraud in 2022, an increase of more than 30 percent over the previous year. Much of this fraud came from fake investing scams and imposter scams. Perhaps most alarming in this report was that there were over 1.1 million reports of identity theft received through the FTC’s IdentityTheft.gov website

The Threats

Organizational Threats - Regulatory and Insurance

- Many compliance related frameworks (FSSCC, NYDFS, FFIEC, SOX)
- Federal and State Regulators
- PII
- State privacy laws and regulations
- International privacy laws and data regulations

- Rising costs
- Higher barriers
  - Not only if you have a control in place
    - What vendor?
- Staff / Contractor training requirements
- “Industry best practices”

Threats

External

Hacitivists

Political / Religious groups

Cyber Criminals

Nation states

Internal

Insider threats

- Commission
- Omission

Supply Chain Vulnerabilities

Misconfigurations

Blind spots

The risks are not always technology

Phishing

- Easy and low cost
  - 3% to 8% will always click
- Open source toolkits are free
- Professional services
- AI based

85% of breaches are based on lost/stolen credentials

Social Engineering

- Exploitation of human nature
- Frequently leads to business process deviation
- Lots of open source tools to aid the attackers

- But there is one threat you are not prepared for and it will cause your organization great harm...

Business Email Compromise (BEC)

- Compromised or well faked email from authorized company personnel
- Financial transactions
- May target:
  - ACH / Wire Transfers
  - Your staff - payroll / benefits
  - Your vendors
  - Your customers!

Deep Fakes

Deep Fakes

Open source AI

Free or near free

No rules

Hard to detect

Artificial Intelligence (AI)

- The artificial is that it, in reality, is just an algorithm
- It does causes people to:
  - Think differently
  - Attack systematically
  - Automate attacks
- Lots of energy is pouring into “AI” attacks
  - Tools
  - Processes
  - Resources
    - Talent
    - Platforms
    - Data

AI / Automation reduces the need for friends

- Single entities can now marshall the same or greater effort than hacking teams
- Automation speeds up the process to
  - Compromise
  - Exploit
  - Cause harm
- Lone wolf attackers have less exposure to operational risks
- Automation will enable the lone wolf attackers to reconnect in the future with even greater scale, effectiveness, and harm

The risks are not always technology

How recent federal moves put your organization at greater risk

- Holding organizations/people accountable
  - Targeting vendors only?
  - What about your organization for not following best practices?
  - Scenario: The vendor released an emergency patch, your organization did not update your systems in a timely manner
    - Does not have to be explicit
- Remember PCI?
  - Started out as a suggestion
  - Currently a big industry with costs and fines
- The recent moves acknowledge the federal government cannot solve the problems
  - It is your turn…

Defeating today’s threats

Obviously the basics / past strategies

- Zero Trust methodologies
- Threat Intelligence
- Stronger Identity solutions
- Faster patch management
- Regular cybersecurity assessments

Combating Deep Fakes

- Do unto them as they do unto us
  - Use their tools and methodologies
- Implement updated business processes
  - Start with finance
  - Think it through from an adversarial perspective
    - You have it right when the insiders cannot break it
- Train everyone on the new processes
  - Start with your CEO
  - Get an explicit commitment
- Empower your people
  - Nature is amazing

Make new friends

Local resources

- National Cyber War Foundation
  - The Arizona Cyber Warfare Range (AZCWR) https://azcwr.org
  - Wisconsin Cyber Threat Response Alliance (WICTRA) htps://wictra.org
  - Michigan Cyber Threat Response Alliance (MICTRA) https://mictra.us
  - Georgia Cyber Warfare Range (GACWR) https://gacwr.org
  - Wyoming is coming online coming soon…
- ISSA / ISC2
- Infragard.org (not .com !)
- National Guard
- Local security meetups