System Security and Vendor Risk Management

Maria S. Thompson
State Chief Risk Officer

NC DIT

WHO NEEDS PASSWORDS?

Starbucks Rewards™

Create a strong password

Password

- ✕ Between 8 and 25 characters
- ✕ At least one number
- ✕ At least one capital letter
- ✕ At least one lowercase letter
- ✕ At least one special character such as exclan or comma

NC DIT

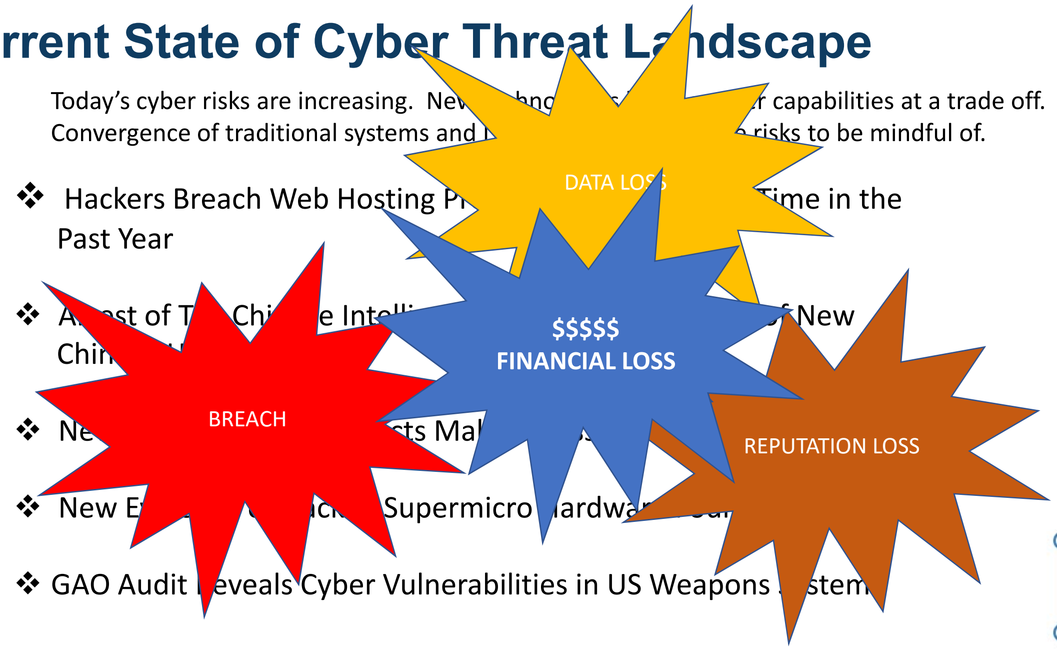
AGENDA

- ❖ Current State Threat Landscape
  - ✓ Phishing
  - ✓ Denial of Service / TDOS
  - ✓ Internet of Things
  - ✓ Cyber Hygiene
- ❖ Why is this important to me?
- ❖ ERP Threat Report Findings
- ❖ Cyber Best Practices
  - ✓ Vendor Risk Management
- ❖ Free Cyber Training Resources
- ❖ Cybersecurity Incident Reporting Requirements
- ❖ Questions?

Current State of Cyber Threat La ndscape

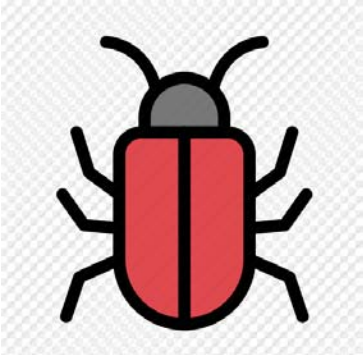
Today’s cyber risks are increasing. Nev hno r capabilities at a trade off.
Convergence of traditional systems and risks to be mindful of.

- ❖ Hackers Breach Web Hosting Pr Time in the Past Year
- ❖ A est of T Chi e Intelli f New Chin
- ❖ Ne ts Mal
- ❖ New E ck Supermicro ardwa
- ❖ GAO Audit eveals Cyber Vulnerabilities in US Weapons stem



Current State of Cyber Threat Landscape

…You are only as strong as the weakest link!



❖ Between 50 – 70% of incoming emails are identified as Phishing, SPAM or Virus

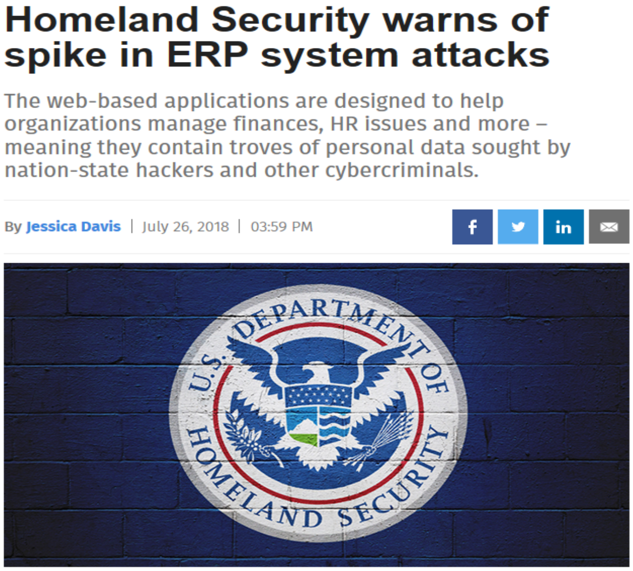
❖ The past couple of years, local counties have reported an uptick in ransomware

❖ There is a reported 133% increase in data breaches reported by first half of 2018 in comparison to previous year

❖ The use of Internet of Things increase daily…along with their associated risks

❖ Business owners continue to accept risks blindly…

WHY IS THIS IMPORTANT TO ME?

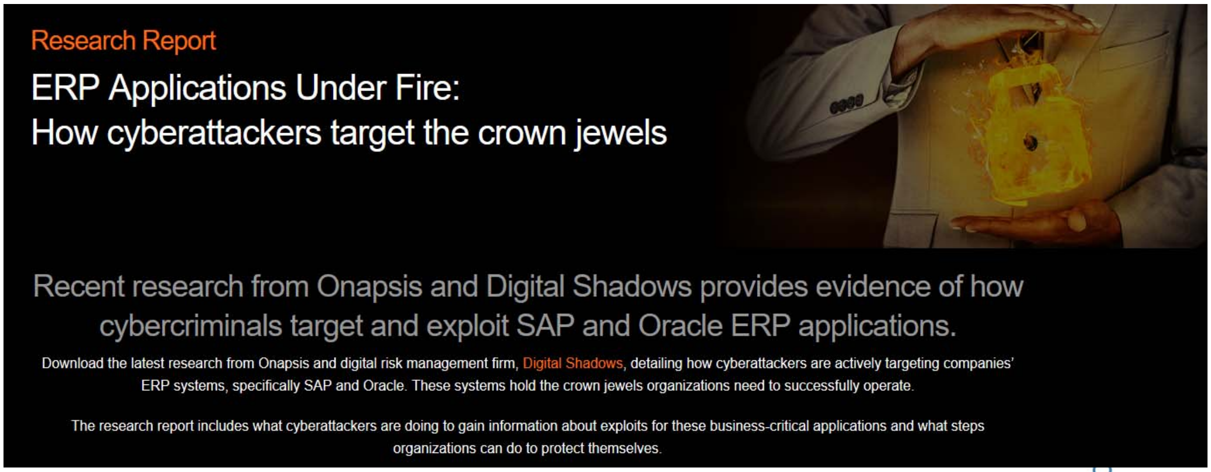


Homeland Security warns of spike in ERP system attacks

The web-based applications are designed to help organizations manage finances, HR issues and more – meaning they contain troves of personal data sought by nation-state hackers and other cybercriminals.

By Jessica Davis | July 26, 2018 | 03:59 PM

ERP Threat Report Findings



Research Report

ERP Applications Under Fire:
How cyberattackers target the crown jewels

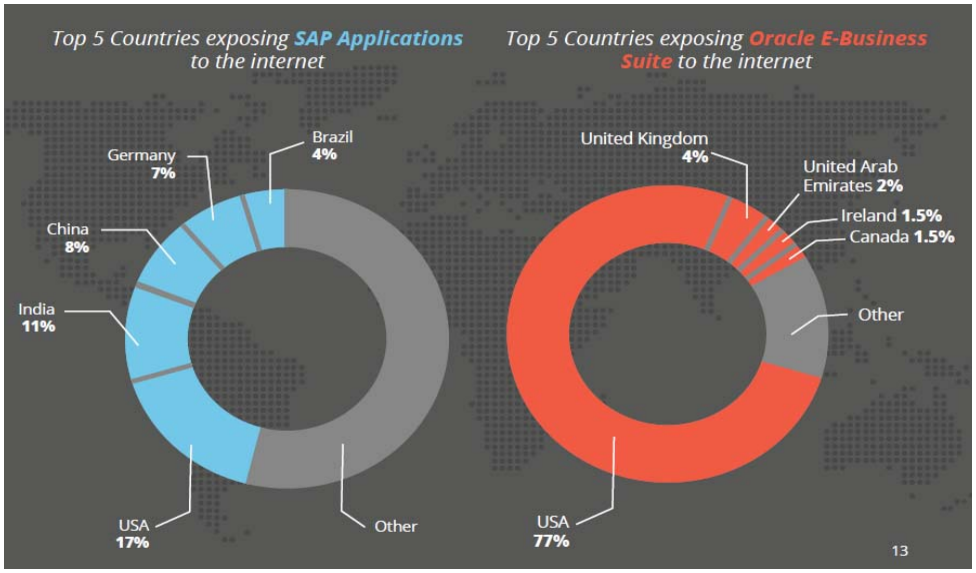
Recent research from Onapsis and Digital Shadows provides evidence of how cybercriminals target and exploit SAP and Oracle ERP applications.

Download the latest research from Onapsis and digital risk management firm, Digital Shadows, detailing how cyberattackers are actively targeting companies' ERP systems, specifically SAP and Oracle. These systems hold the crown jewels organizations need to successfully operate.

The research report includes what cyberattackers are doing to gain information about exploits for these business-critical applications and what steps organizations can do to protect themselves.

"This goes in hand with an observed 100 percent increase of public exploits for SAP and Oracle ERP applications over the last three years, and a 160 percent increase in the activity and interest in ERP-specific vulnerabilities from 2016 to 2017," the report found."

ERP Threat Report Findings – ERP Footprint



ERP Threat Report Findings

These vulnerabilities affect both SAP and Oracle ERP systems. The key findings were:

- Hacktivist groups are actively attacking ERP applications to disrupt critical business operations and penetrate target organizations
- Cybercriminals have evolved malware to target internal, “behind-the-firewall” ERP applications.
- Nation-state sponsored actors have targeted ERP applications for cyber espionage and sabotage
- Attacks vectors are evolving, still mainly leveraging known ERP vulnerabilities vs. zero-days
- Cloud, mobile and digital transformations are rapidly expanding the ERP attack surface, and threat actors are taking advantage.
- Leaked information by third parties and employees can expose internal ERP applications

ERP Threat Report Findings

- “attackers could target one of thousands of ERP vulnerabilities, therefore making it crucial for organizations to prioritize and address ERP vulnerabilities as they would any other existing production application.”

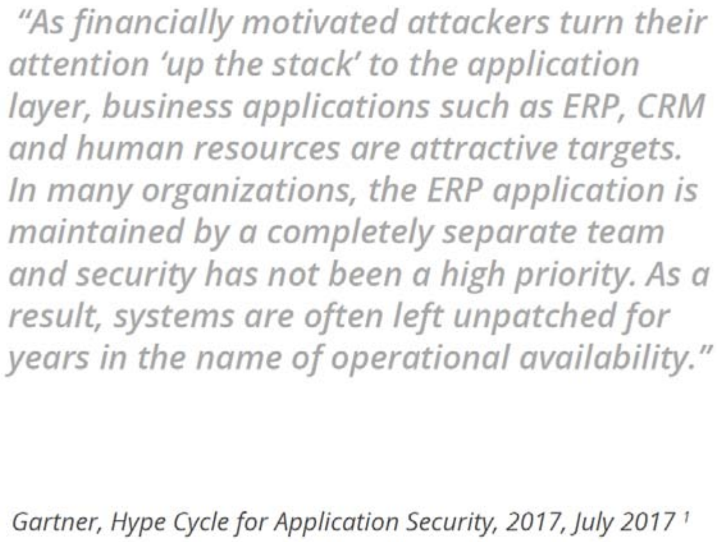
- “The biggest risk for organizations is not knowing the risks. Organizations must ensure the right level of governance around cyber risks that could affect ERP applications..
  - ✓ Visibility and proactive management of potential vulnerabilities and risks affecting ERP applications
  - ✓ Non-production systems are higher risks…less security controls or audits

ERP Threat Report Findings

- “Moving your ERP applications to the cloud will not transfer accountability and your organization is still responsible for the data hosted and processed by those applications. ERP customers still need to address security in cloud environments, to ensure the data is safe.”

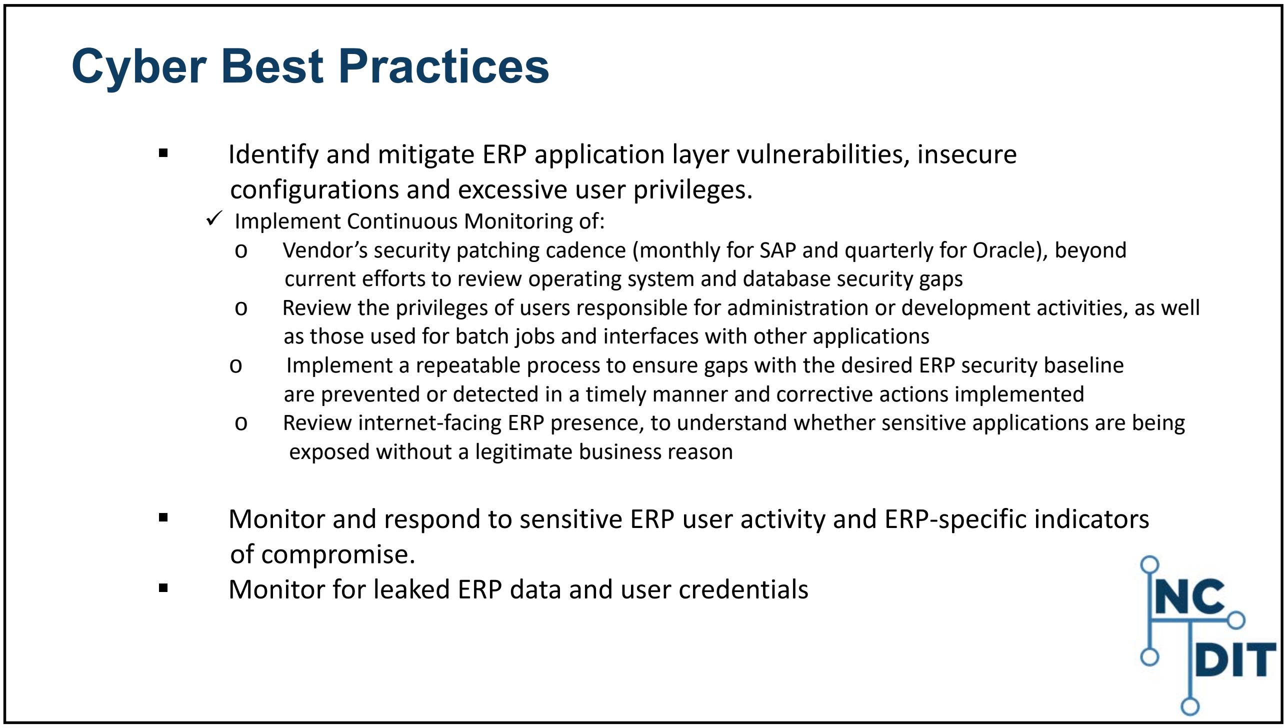
Note: DHS sent out an alert to notify large organizations about these threat due to the nature of the evidence identified. **There is clear evidence of intent from threat actors to target ERP applications,** so organizations must be aware of this and be able to prevent a breach by following the recommended protocols.

Cyber Best Practices



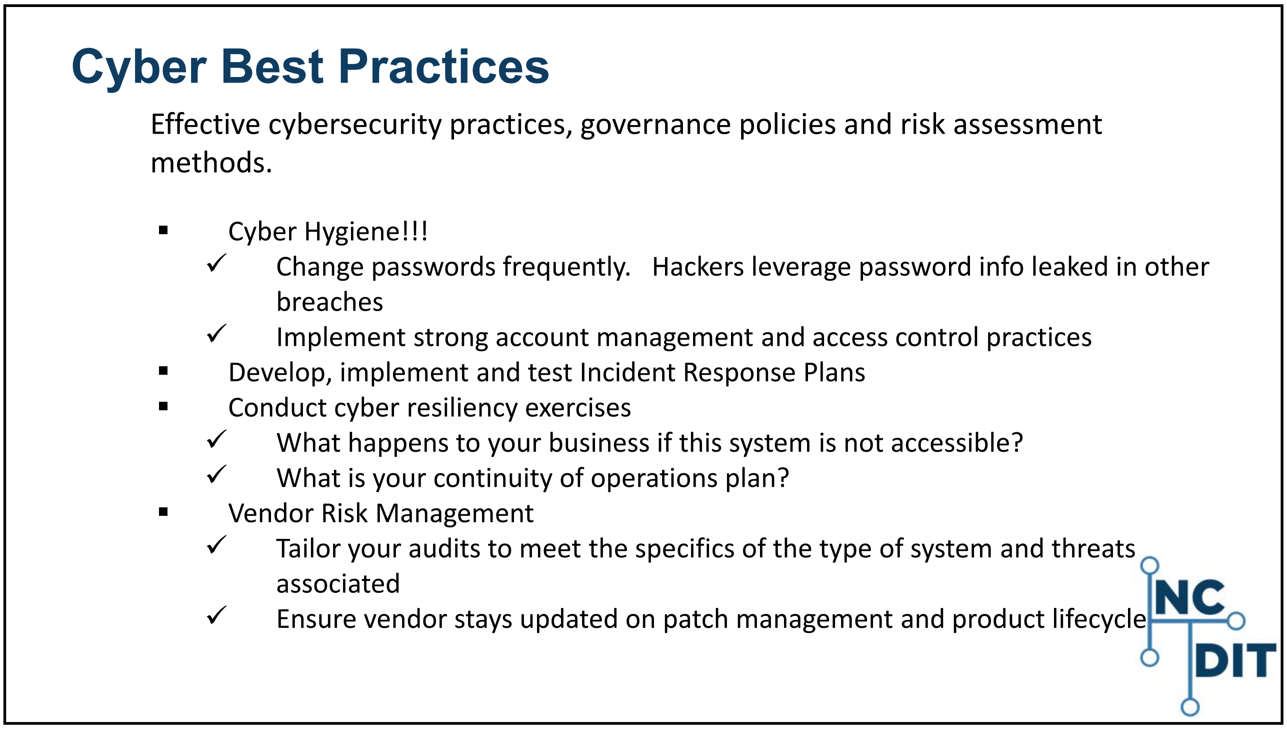
“As financially motivated attackers turn their attention ‘up the stack’ to the application layer, business applications such as ERP, CRM and human resources are attractive targets. In many organizations, the ERP application is maintained by a completely separate team and security has not been a high priority. As a result, systems are often left unpatched for years in the name of operational availability.”

Gartner, Hype Cycle for Application Security, 2017, July 2017 [1]



Cyber Best Practices

- Identify and mitigate ERP application layer vulnerabilities, insecure configurations and excessive user privileges.
  - ✓ Implement Continuous Monitoring of:
    - o Vendor’s security patching cadence (monthly for SAP and quarterly for Oracle), beyond current efforts to review operating system and database security gaps
    - o Review the privileges of users responsible for administration or development activities, as well as those used for batch jobs and interfaces with other applications
    - o Implement a repeatable process to ensure gaps with the desired ERP security baseline are prevented or detected in a timely manner and corrective actions implemented
    - o Review internet-facing ERP presence, to understand whether sensitive applications are being exposed without a legitimate business reason
- Monitor and respond to sensitive ERP user activity and ERP-specific indicators of compromise.
- Monitor for leaked ERP data and user credentials



Cyber Best Practices

Effective cybersecurity practices, governance policies and risk assessment methods.

- Cyber Hygiene!!!
  - ✓ Change passwords frequently. Hackers leverage password info leaked in other breaches
  - ✓ Implement strong account management and access control practices
- Develop, implement and test Incident Response Plans
- Conduct cyber resiliency exercises
  - ✓ What happens to your business if this system is not accessible?
  - ✓ What is your continuity of operations plan?
- Vendor Risk Management
  - ✓ Tailor your audits to meet the specifics of the type of system and threats associated
  - ✓ Ensure vendor stays updated on patch management and product lifecycle

Free Cybersecurity Training Resources

Federal Virtual Training Environment (FedVTE)

□ Course proficiency ranges from beginner to advanced levels. Several courses align with a variety of IT certifications such as Certified Information Systems Security Professional (CISSP), CISA, CEH, Pen Testing etc.

- ✓ https://niccs.us-cert.gov/training/fedvte

□ National Initiative for Cybersecurity Careers and Studies

- ✓ https//niccs.us-cert.gov/formal-education

Let's Connect!

@NCDIT
@BroadbandIO
@ncicenter

NC Department of Information Technology

NCDIT

NC DIT

@NCDIT

it.nc.gov