Cybersecurity and Risk Management North Carolina Public Schools

Joint Legislative Education Oversight Committee
March 6, 2018
Phil Emer

NC STATE UNIVERSITY

THE WILLIAM & IDA
FRIDAY INSTITUTE
FOR EDUCATIONAL INNOVATION

Agenda

- A little background
- Progress on implementation of §7.23A of the 2017 budget
- Understanding cybersecurity threats to NC public schools
- Next steps in protecting NC schools

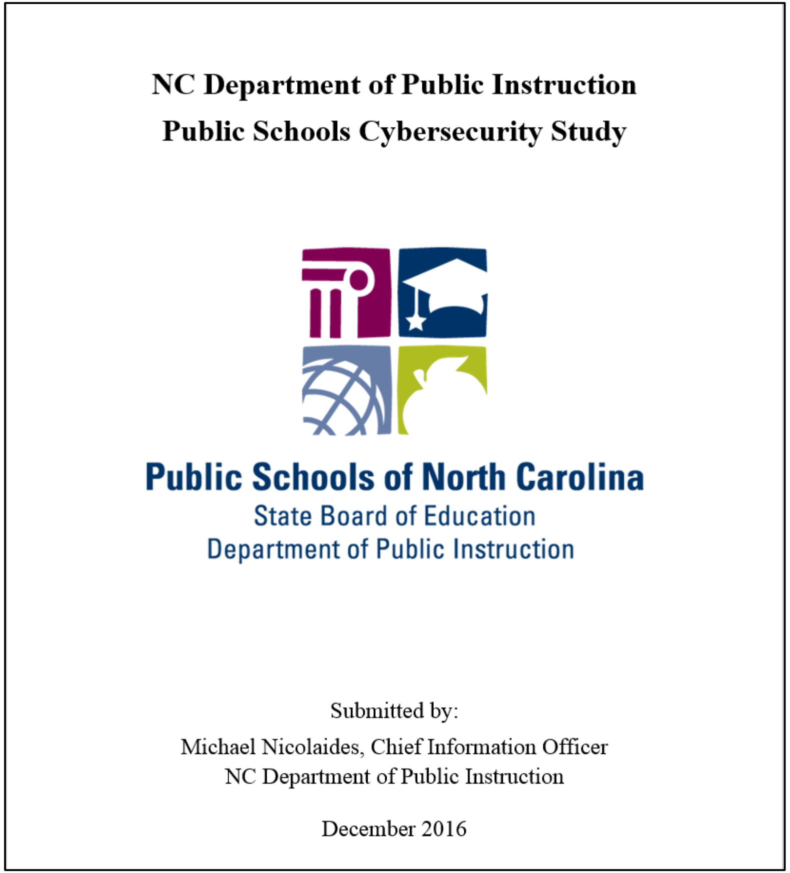
The NC School Connectivity Initiative (SCI)

- Established in S.L. 2007-323 §7.28
- Delivers reliable tier one Internet Access to LEAs and Charter Schools
- Supports fiber connectivity to virtually every public school in NC
- Supports digital learning ready WiFi connectivity at the classroom level
- Coordinates LEA interactions with the Federal E-rate discount program
- $31M appropriation leveraged against $57M in E-rate receipts in 2017
- Provides a client network engineering service (CNE) to LEAs and charter schools to advise and consult on network design, operations, troubleshooting

2016 Public Schools Cybersecurity Study

Findings

- Schools vary significantly in their portfolios of cybersecurity capacity
- Small school districts and charter schools are the most vulnerable
- **The majority of school districts and charter schools surveyed are not prepared for a significant disaster or cybersecurity event**
- Loss of federal funding for Internet content filtering and firewall services
- School districts and charter schools are not mandated to follow guidelines outlined in the North Carolina Statewide Information Security Manual



NC Department of Public Instruction

Public Schools Cybersecurity Study

Public Schools of North Carolina
State Board of Education
Department of Public Instruction

Submitted by:

Michael Nicolaides, Chief Information Officer
NC Department of Public Instruction

December 2016

LEA Technology Directors and staff do an amazing job in one of the most challenging IT landscapes.

Progress on §7.23A of S.L. 2017-57

S.L. 2017-57, SECTION 7.23A appropriates $200,000 in each year of the biennium to ***Expand School Connectivity Initiative/Cybersecurity and Risk Management***

The State Board of Education and the Department of Public Instruction, in collaboration with the Friday Institute at North Carolina State University, shall expand the School Connectivity Initiative client network engineering to include cybersecurity and risk management services supporting local school administrative units and charter schools. The expansion shall include the following:

*(1) **Continuous monitoring and risk assessment.** – Cloud-based solutions to discover assets, assess their security posture, and recommend corrective actions based on real-world risk reduction.*

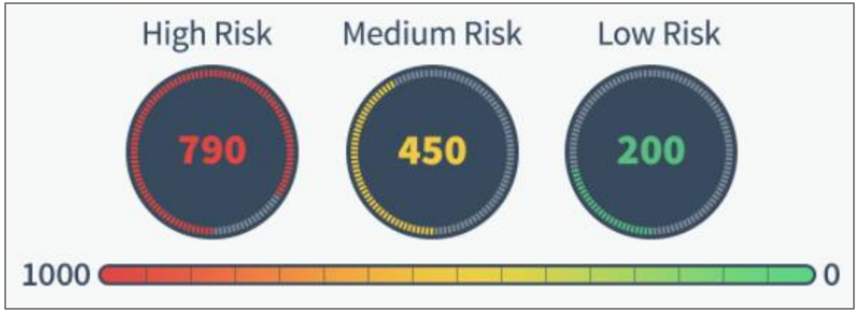
*(2) **Security advisory and consulting services.** – Five regional security consultants working with schools to assess security posture and develop and implement improvement plans. The plans shall include security policy, building security programs, implementing effective security controls, and ongoing support for operating security governance.*

*(3) **Security training and education services.** – Security training and education for teachers, staff, and administrators.*

The Directive

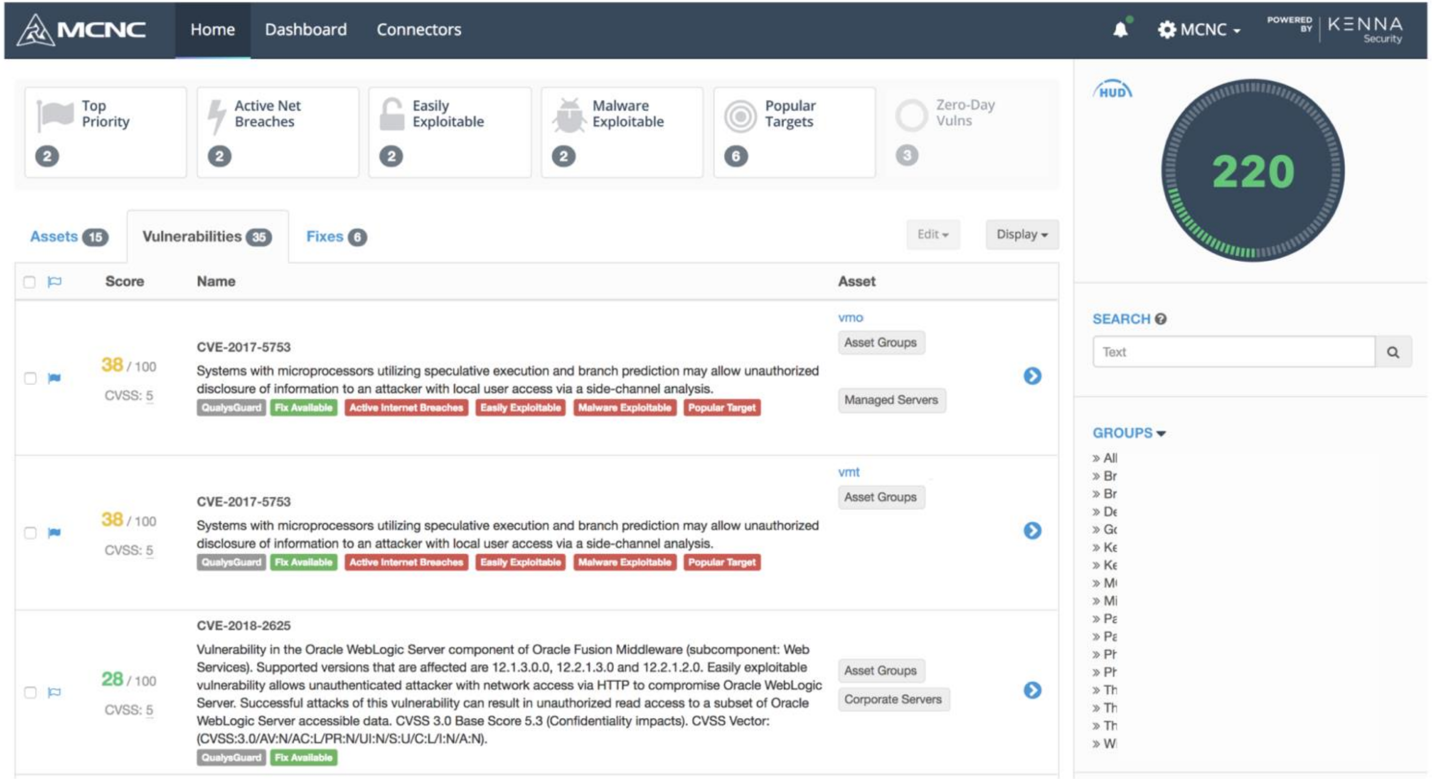
- **Continuous monitoring and risk assessment.** – Cloud-based solutions to discover assets, assess their security posture, and recommend corrective actions based on real-world risk reduction. [$200K]
- **Security advisory and consulting services.** – Five regional security consultants working with schools to assess security posture and develop and implement improvement plans. The plans shall include security policy, building security programs, implementing effective security controls, and ongoing support for operating security governance.
- **Security training and education services.** – Security training and education for teachers, staff, and administrators.

Continuous Monitoring and Risk Assessment Service



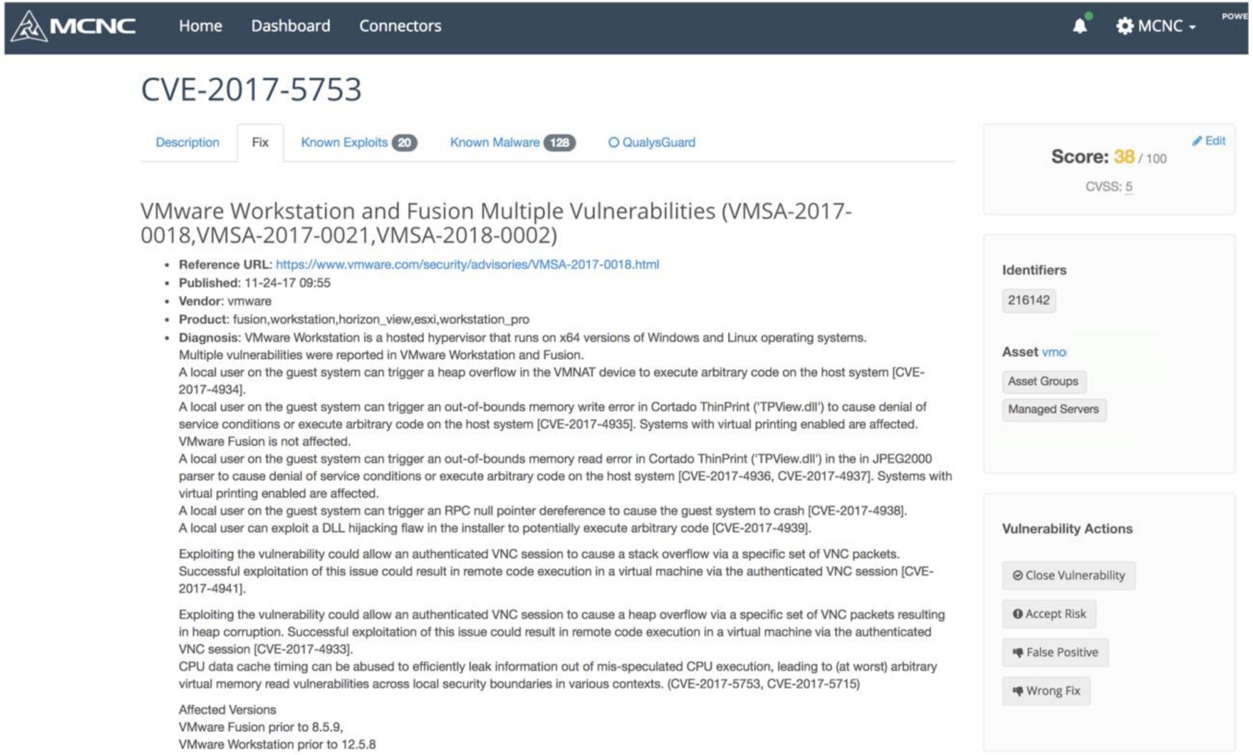
- MCNC CNE manages setup, configuration, and operation of continuous, automated scanning of IT systems for the presence of vulnerabilities.
- LEA admins access a web portal that presents live vulnerability data.
- Vulnerability data enriched with external threat intelligence.
- Identified issues are prioritized based on risk to LEA.
- Admins see issues that need attention and get details on how to remediate.
- Risk scores improve as issues are addressed.

Identify Vulnerabilities and Risk



Score	Name	Asset
38 / 100 CVSS: 5	CVE-2017-5753 Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. QualysGuard Fix Available Active Internet Breaches Easily Exploitable Malware Exploitable Popular Target	vmo Asset Groups Managed Servers
38 / 100 CVSS: 5	CVE-2017-5753 Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. QualysGuard Fix Available Active Internet Breaches Easily Exploitable Malware Exploitable Popular Target	vmt Asset Groups
28 / 100 CVSS: 5	CVE-2018-2625 Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). QualysGuard Fix Available	Asset Groups Corporate Servers

Apply Fixes



CVE-2017-5753

VMware Workstation and Fusion Multiple Vulnerabilities (VMSA-2017-0018,VMSA-2017-0021,VMSA-2018-0002)

- **Reference URL:** https://www.vmware.com/security/advisories/VMSA-2017-0018.html
- **Published:** 11-24-17 09:55
- **Vendor:** vmware
- **Product:** fusion,workstation,horizon_view,esxi,workstation_pro
- **Diagnosis:** VMware Workstation is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems.
  Multiple vulnerabilities were reported in VMware Workstation and Fusion.
  A local user on the guest system can trigger a heap overflow in the VMNAT device to execute arbitrary code on the host system [CVE-2017-4934].
  A local user on the guest system can trigger an out-of-bounds memory write error in Cortado ThinPrint ('TPView.dll') to cause denial of service conditions or execute arbitrary code on the host system [CVE-2017-4935]. Systems with virtual printing enabled are affected. VMware Fusion is not affected.
  A local user on the guest system can trigger an out-of-bounds memory read error in Cortado ThinPrint ('TPView.dll') in the in JPEG2000 parser to cause denial of service conditions or execute arbitrary code on the host system [CVE-2017-4936, CVE-2017-4937]. Systems with virtual printing enabled are affected.
  A local user on the guest system can trigger an RPC null pointer dereference to cause the guest system to crash [CVE-2017-4938].
  A local user can exploit a DLL hijacking flaw in the installer to potentially execute arbitrary code [CVE-2017-4939].

  Exploiting the vulnerability could allow an authenticated VNC session to cause a stack overflow via a specific set of VNC packets. Successful exploitation of this issue could result in remote code execution in a virtual machine via the authenticated VNC session [CVE-2017-4941].

  Exploiting the vulnerability could allow an authenticated VNC session to cause a heap overflow via a specific set of VNC packets resulting in heap corruption. Successful exploitation of this issue could result in remote code execution in a virtual machine via the authenticated VNC session [CVE-2017-4933].
  CPU data cache timing can be abused to efficiently leak information out of mis-speculated CPU execution, leading to (at worst) arbitrary virtual memory read vulnerabilities across local security boundaries in various contexts. (CVE-2017-5753, CVE-2017-5715)

  Affected Versions
  VMware Fusion prior to 8.5.9,
  VMware Workstation prior to 12.5.8

Score: 38 / 100

CVSS: 5

Identifiers

216142

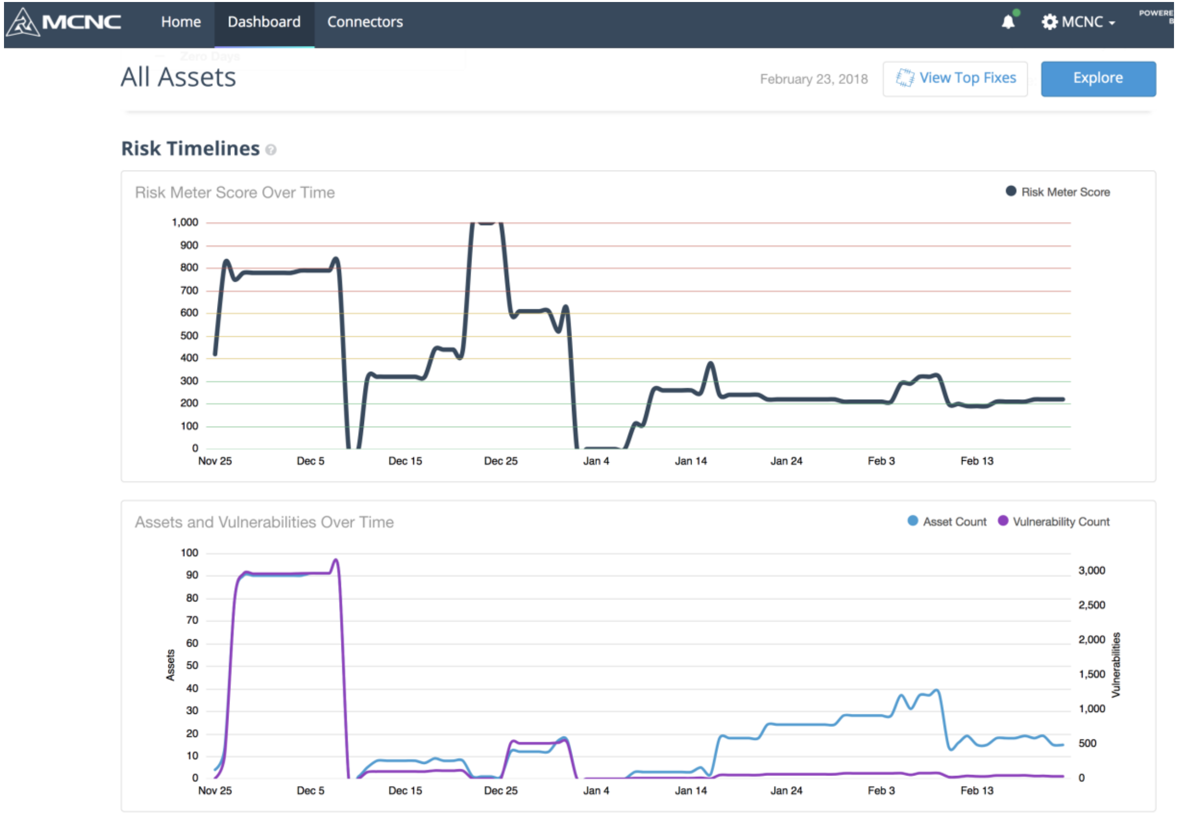
Asset vmo

Asset Groups

Managed Servers

Vulnerability Actions

Continuously Monitor Vulnerabilities and Risk



All Assets

February 23, 2018

Risk Timelines

Risk Meter Score Over Time

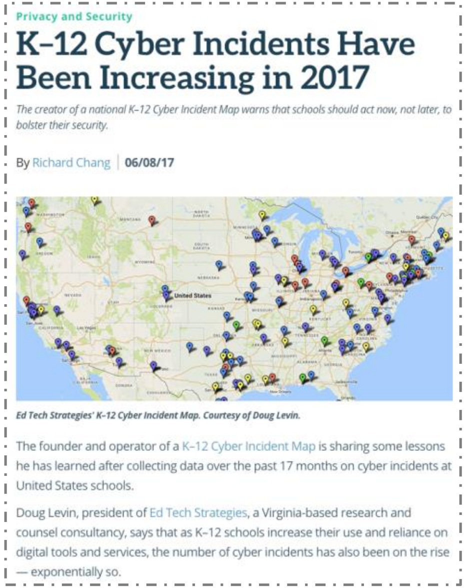
Assets and Vulnerabilities Over Time

Continuous Monitoring and Risk Assessment Service

- **$200k funding provided in current budget provision will cover cost to include *external* network scanning for all K-12 LEAs and Charters.**
- Technical Development Complete
- Currently in Beta Testing
- Testing with 3 K-12 School Systems
- Will add more systems in coming weeks
- Once testing is complete in Spring 2018, we will begin rolling the service out to all NC LEAs and Charter Schools.
- In Summer 2018 we will begin enhancing the service to allow scanning of *internal* school networks – costs will increase with more internal systems

Understanding the Threat Landscape

Attackers are Specifically Targeting K-12 Schools



Privacy and Security

K–12 Cyber Incidents Have Been Increasing in 2017

The creator of a national K–12 Cyber Incident Map warns that schools should act now, not later, to bolster their security.

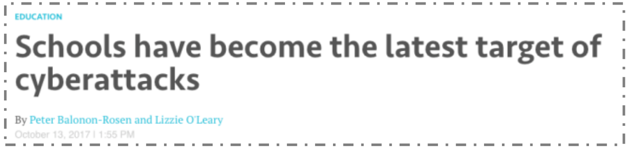
By Richard Chang | 06/08/17

Ed Tech Strategies' K–12 Cyber Incident Map. Courtesy of Doug Levin.

The founder and operator of a K–12 Cyber Incident Map is sharing some lessons he has learned after collecting data over the past 17 months on cyber incidents at United States schools.

Doug Levin, president of Ed Tech Strategies, a Virginia-based research and counsel consultancy, says that as K–12 schools increase their use and reliance on digital tools and services, the number of cyber incidents has also been on the rise — exponentially so.

1



EDUCATION

Schools have become the latest target of cyberattacks

By Peter Balonon-Rosen and Lizzie O'Leary

October 13, 2017 | 1:55 PM

2

Department of Education: Hackers are now targeting elementary and high schools

Abigail Hess | @AbigailJHess | 4:28 PM ET Tue, 24 Oct 2017

Hill Street Studios | Getty Images

Even elementary schools have been attacked by cyber criminals.

No one is safe from a cyber attack, not even elementary school children.

3

US schools are uniquely vulnerable to cyber attacks

By Ian Barker | Published 2 months ago

2 Comments

A new study by application delivery and security company Radware reveals that US schools are uniquely vulnerable to the threat of cyber attacks.

4

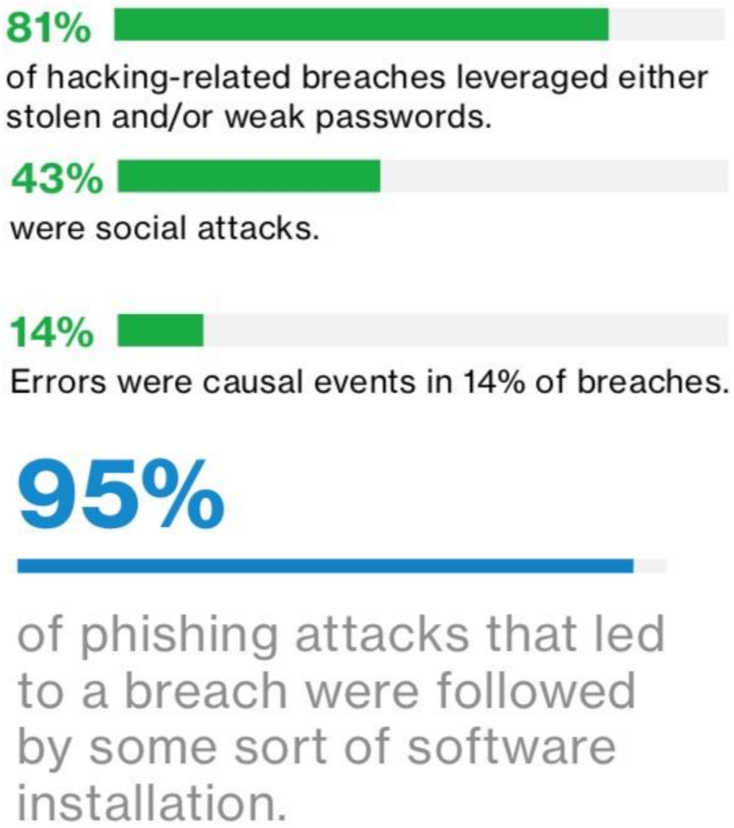
Some NC Schools Attacks

- LEA contacted MCNC CNE after suffering Ransomware attack.
- No backups or recovery options in place. LEA was forced to rebuild most of internal infrastructure just 2 weeks prior to the start of school.
- LEA lacked even the most basic security controls. Poor cyber hygiene led to ransomware compromise.

- 3 different LEAs contacted MCNC CNE for assistance to address persistent malware reinfections. Dozens of devices spanning multiple sites re-infected with malware over and over again.
- Implementation of good cyber hygiene practices could have saved hundreds of hours and hundreds of thousands of dollars in recovery efforts.

Common Attacks

- **Malware** - Viruses, Worms, Ransomware
- **Phishing** - Enticing users to click on malware
- **Database Attacks** - Exfiltrating info from a database using vulnerabilities in the server/database
- **Cross-Site Scripting** - Attacking users of a website by posting malicious content that affects other user’s browser
- **Denial of Service** - Preventing the legitimate use of a website or service by bombarding it with “fake” requests
- **Session Hijacking** - Attacks on the network between the user and the server to gain access to information or impersonate the user
- **Credential Reuse** - Finding weak passwords through attack or discovering passwords through other means



81%

of hacking-related breaches leveraged either stolen and/or weak passwords.

43%

were social attacks.

14%

Errors were causal events in 14% of breaches.

95%

of phishing attacks that led to a breach were followed by some sort of software installation.

Source: Rapid7 and Verizon Data Breach Investigations Report 2017

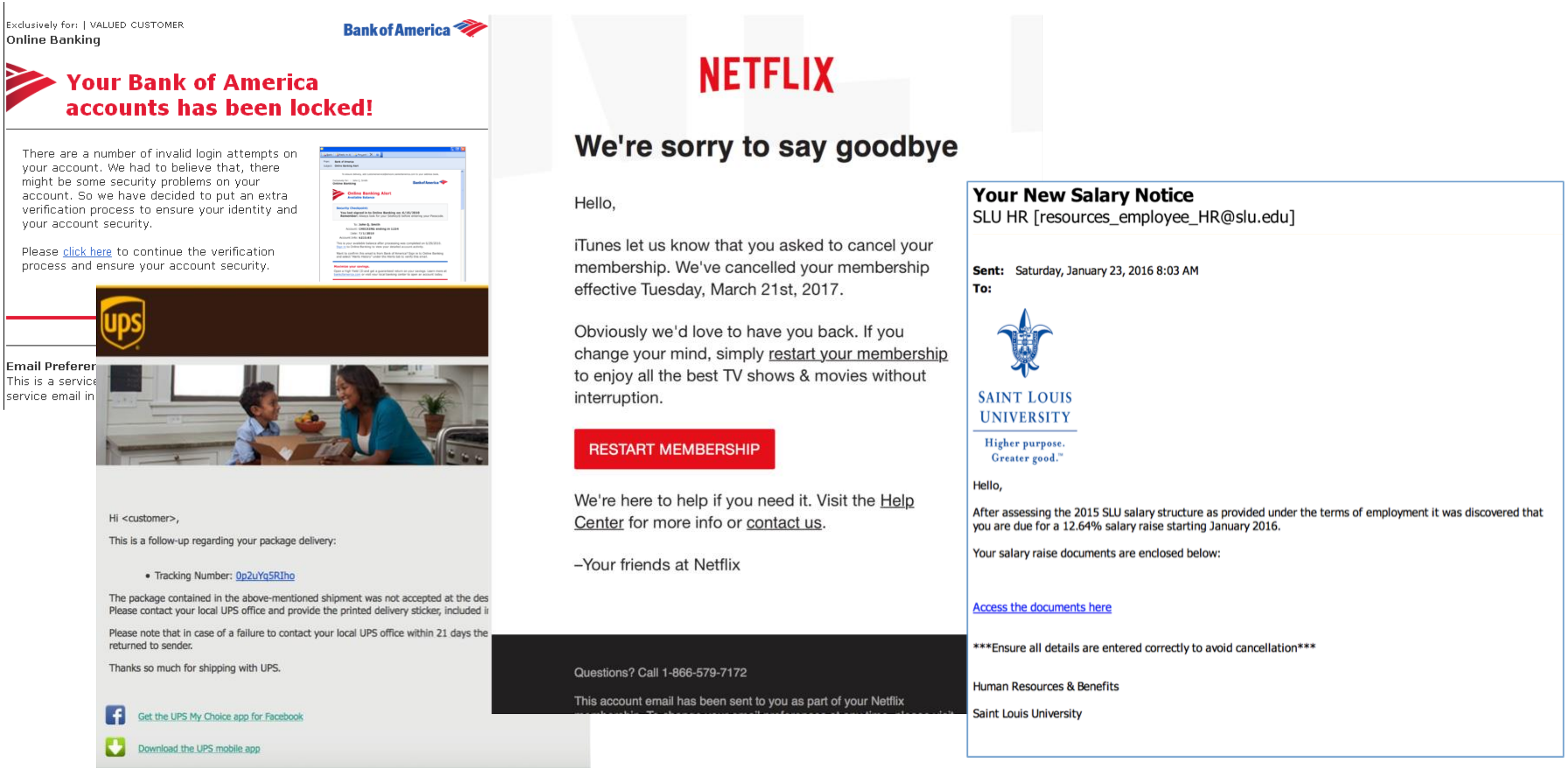
Phishing - Hand in hand with Malware

Threat to NC Schools

- Often leads to ransomware exploits or credential stealing for sensitive systems with financial data.
- Likely the largest single threat as it pervasive, easy, inexpensive and it works frequently.
- This is the most common form of social engineering. Well-crafted emails are now very difficult to flag as fake.

Actions to Mitigate

- ✓ Increase content filtering capabilities
- ✓ Use cloud-based e-mail systems with integrated threat intelligence
- ✓ **Train users continually**
- ✓ Ensure passwords are secure
- ✓ Use single-sign-on technology to limit the number of passwords users must remember



Exclusively for: | VALUED CUSTOMER
Online Banking

Bank of America

Your Bank of America accounts has been locked!

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Please click here to continue the verification process and ensure your account security.

Email Preferer
This is a service
service email in

ups

Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: 0p2uYq5RIho

The package contained in the above-mentioned shipment was not accepted at the des
Please contact your local UPS office and provide the printed delivery sticker, included i

Please note that in case of a failure to contact your local UPS office within 21 days the
returned to sender.

Thanks so much for shipping with UPS.

Get the UPS My Choice app for Facebook

Download the UPS mobile app

NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

Your New Salary Notice
SLU HR [resources_employee_HR@slu.edu]

Sent: Saturday, January 23, 2016 8:03 AM
To:

SAINT LOUIS UNIVERSITY
Higher purpose. Greater good.™

Hello,

After assessing the 2015 SLU salary structure as provided under the terms of employment it was discovered that you are due for a 12.64% salary raise starting January 2016.

Your salary raise documents are enclosed below:

Access the documents here

Ensure all details are entered correctly to avoid cancellation

Human Resources & Benefits

Saint Louis University

Are these legitimate emails?

Protecting NC Public Schools

Security Services Already in Place through SCI

DDoS Attacks in 2017

420

DDoS Attacks on NCREN

100 %

of Attacks Remediated

MCNC DDoS protection and mitigation

zscaler™

Web security

NCEdCloud IAM

Single User ID
and Password

NC DIT

Firewall services

KENNA Security

Continuous monitoring
and risk assessment

We Will Never Be 100% “Secure” - So Be Prepared

Mitigate When Possible

Identify most likely threats and prioritize remediation.

Use updated, modern, cloud-based services.

Keep software up to date.

Continually train users.

Detect Early

Government entities are generally slower than the private sector in detecting breaches.

Early detection can prevent loss of data and disruption to services.

Monitor network and systems closely.

Limit Recovery Time

Have a response plan.

Train staff to identify suspicious behavior and report quickly.

Maintain backups.

Use cloud-based services that include backup natively.

Summary of Suggested Actions for NC Public Schools

Educate Users	● Enhance training for LEA and charter staff ● Additional training programs for students and teachers
Monitor & Detect	● Increase CNE & detection capabilities ● Security survey of all districts
Prevent Denial of Service	● **MCNC DDOS mitigation services address this**
Minimize Exposure Footprint	● Use modern, cloud-based services ● Opt for Software as a Service (SaaS)
Minimize Recovery Time	● Build a statewide security framework template ● Ensure critical systems are backed-up frequently

Security Advisory Services

- LEAs need assistance to assess and improve cybersecurity programs, and to assist in responding to incidents. The threat is real and growing.
- There is no magic bullet.
- Each LEA needs a baseline security assessment to set a path forward for improving their cybersecurity risk posture.
- Based on demonstrated success with SCI CNE technology consulting team, we believe a similar approach to providing cybersecurity consulting resources can optimize cost and opportunity for success.
- The SCI CNE program should be enhanced with cybersecurity consultants to provide assistance to NC LEAs and charter schools.
- Funding on the front end helps contain the substantial incident response costs.

Acknowledgements

Michael Nicolaides, CIO, NCDPI
KC Hunt, Chief information security officer, NCDPI
Ray Zeisz, Director enterprise infrastructure programs, Friday Institute
Jean Davis, CEO, MCNC
Dave Furiness, Director client network engineering, MCNC
Chris Beal, Chief Information Security Officer, MCNC

Questions

Phil Emer
Director Technology Planning and Policy
The Friday Institute
paemer@ncsu.edu