NEW HAMPSHIRE MUNICIPAL ASSOCIATION

NHMA 75 1941-2016
NEW HAMPSHIRE MUNICIPAL ASSOCIATION
Celebrating Seventy-Five Years of Service to Your Hometown

The Growing Threat of Ransomware

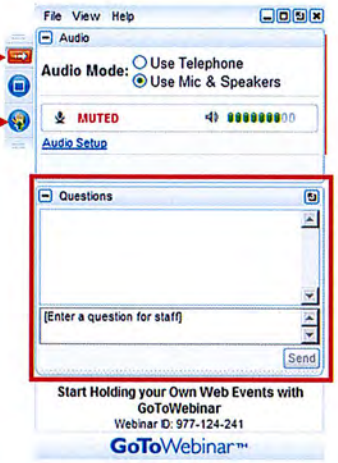
Presented by:

Erin Makarow, Marketing Coordinator, RMON Networks
David Cohen, Senior Services Manager RMON Networks
Chris Chaves, Senior Sales Engineer, Sophos

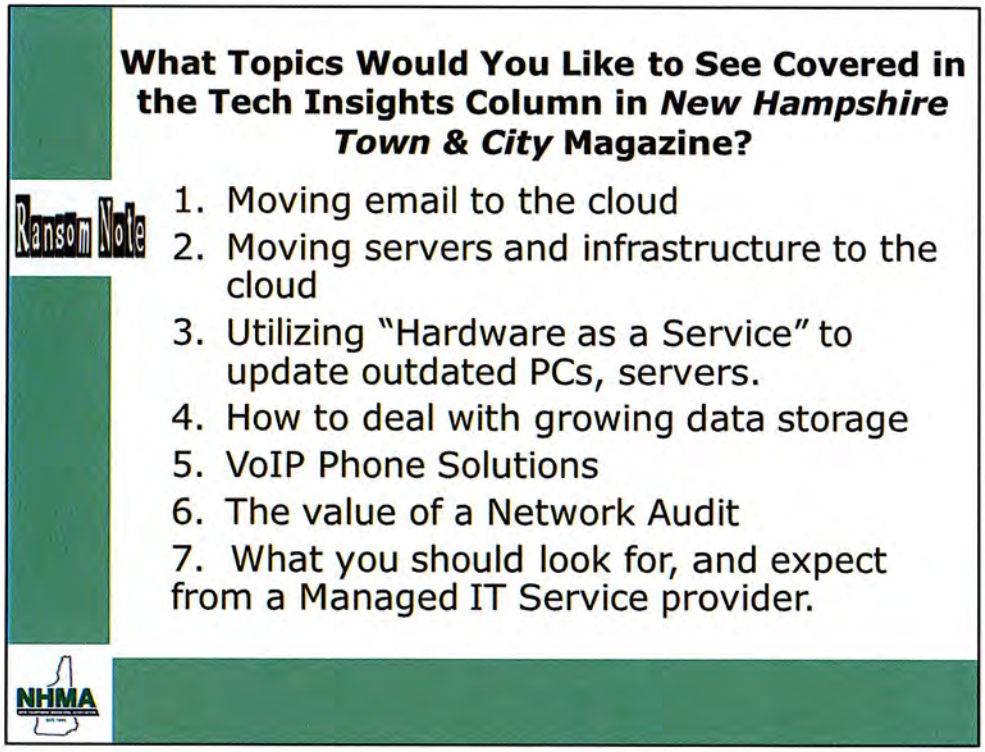
October 12, 2016

How to Participate Today

- Open and close your Panel
- Submit text questions
- Couple of questions for today
- Q&A addressed at the end of today's and/or during session at presenter's discretion

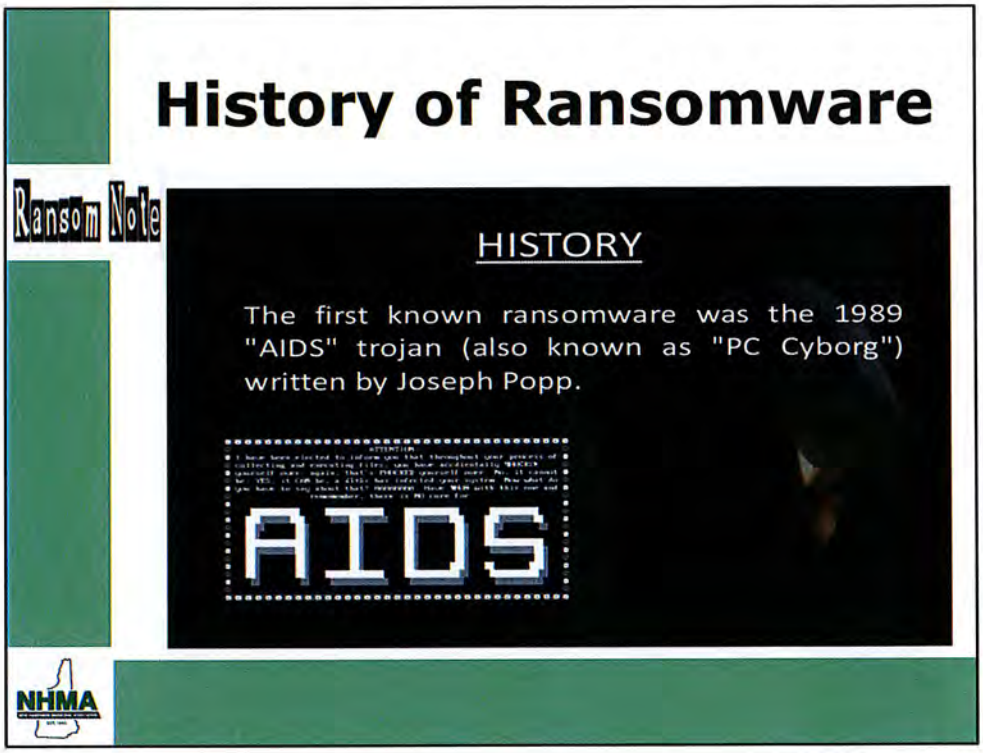


My name is Erin Makarow, and I am the Marketing Coordinator for RMON Networks. If you haven't heard of RMON Networks, we have been providing I.T. Services to Municipalities since 2002, and we have been fortunate to be working with the NH Municipality Association for several years now. Last year I had approached Tim Fortier at the NHMA just shortly after the media started reporting that the Town of Tewksbury, MA P.D. had contracted ransomware. The Tewksbury PD was not prepared to combat this virus at all, and ended up paying the ransomware. It was a very public event. I hate hearing stories like that one, I feel like there is so many ways we can help. So I thought.. You know.. I am going to call Tim at the NHMA, and ask if there was something I could do to help make Towns aware of this issue... so to make a long story short, RMON Networks has been writing the Tech Insights column for the NHMA's Town and City Magazine for a little over a year now. Back then it started with a ransomware article, and now here we are... talking about this growing threat in more depth.



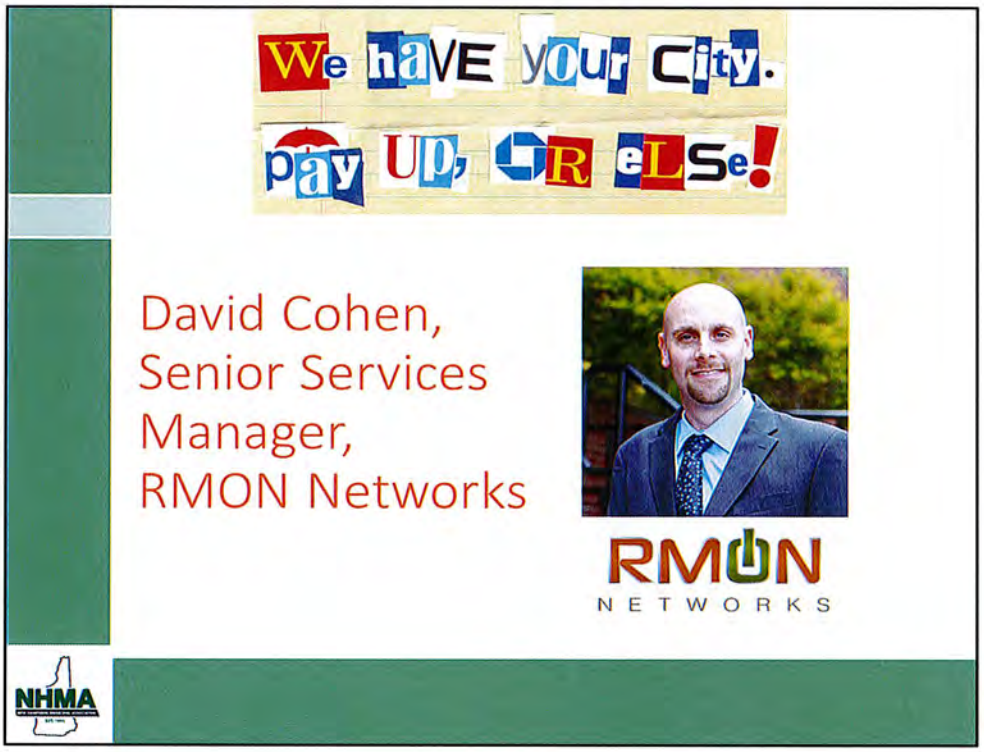
Before we begin. I was to take a quick poll from our audience. What other technology topic would you like to see featured in Town and City Magazine?

Before we jump right in here, I just wanted to stop and point out that October is cyber security awareness month. So we really picked a perfect month to all gather here and talk about ransomware.

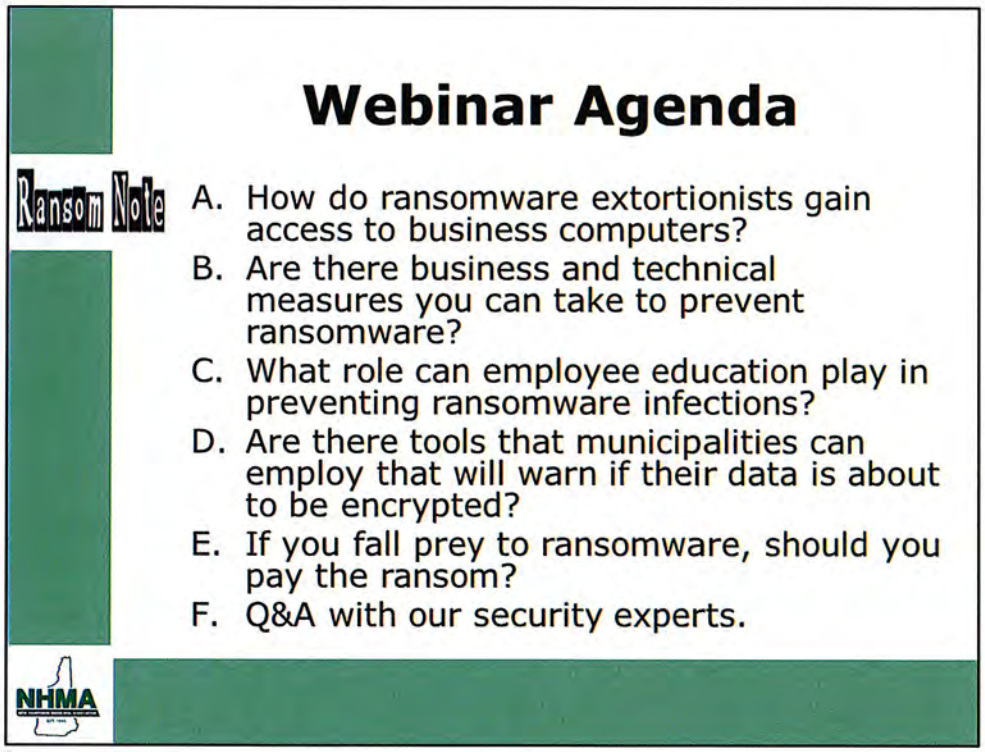


1st piece of ransomware was written in 1985, it was a Trojan called the Aids Trojan or PC Cyborg, it encrypted data on a hard disk, and physically asked people to send money through the US mail. Does anyone else see the problem with this???? We know where they are, we have their address! Since it was easily traceable because we had a physical address, the concept of ransomware didn't evolve. BUT when bitcoin came about, the playing field really changed. This is when ransomware revolutionized cyber crime, and has recently been reported as the most profitable scam in history. AND nobody is immune, agencies, and entities of all sizes have been reported victims with incidents escalating at an alarming rate. The FTC reports incidents quadrupling this year alone to on average 4,000 a DAY. Ransomware will continue

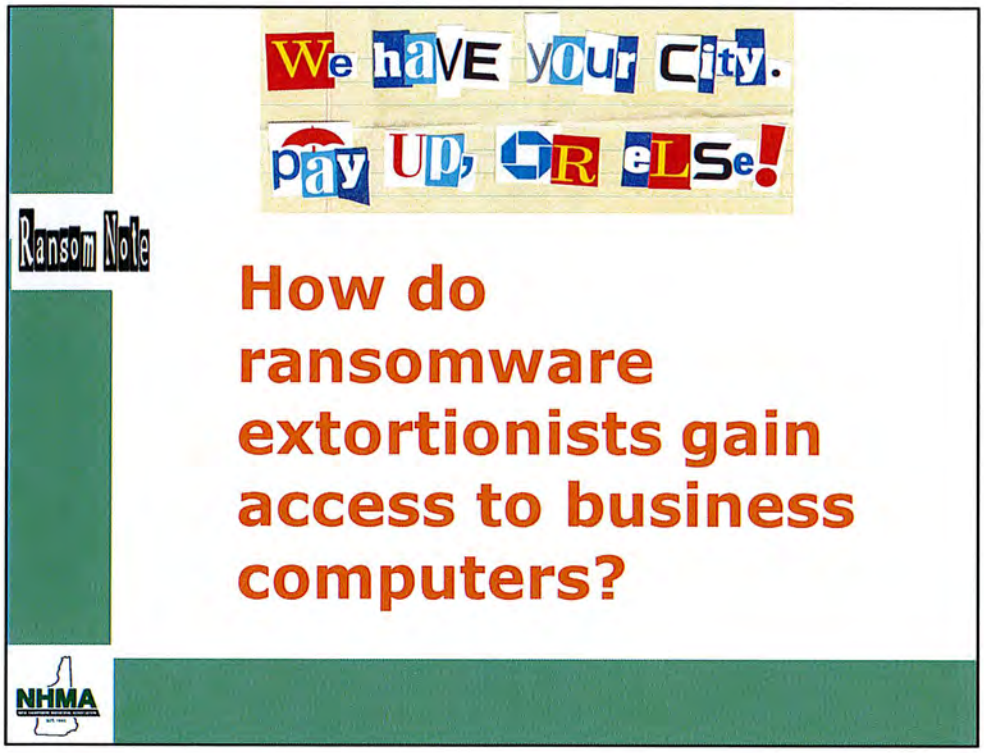
You may ask yourself why would a local government office be a target? Ironically, as I was creating this presentation the owner came over and dropped the latest edition of of GCN Magazine on my desk. It's a technology for government focused magazine. Ransomware targeting governments was this months main focus. Here you can see a power message they are delivering. Here you are being described as "easy pickings". Why are you easy pickings? According to GCN Magazine, most agencies do not have the technology currently in place, and are not prioritizing the technology in their budget. We want you to know that there are programs an products out there, that you can implement within a smaller, planned budget. AND Hopefully you will have many takeaways from today's presentation to get you started.



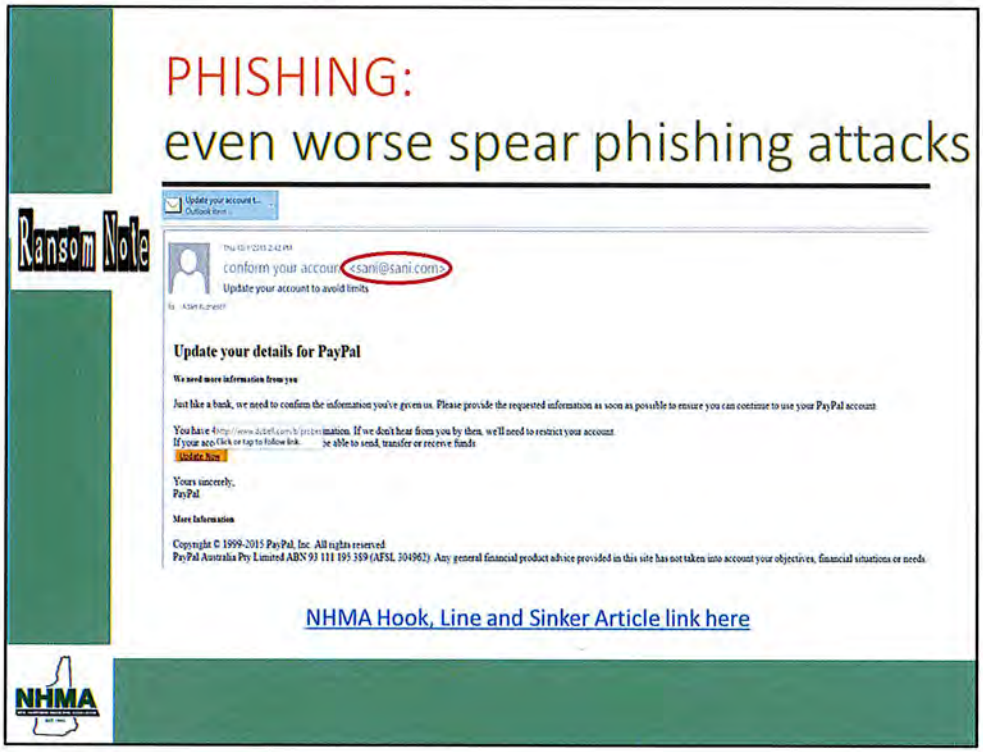
At this point I am going to hand this presentation over to David Cohen, David is our extremely talented service manager here at RMON Networks. David Cohen has over 2 decades of industry experiences and too many certifications to list with Microsoft, Dell, Citrix, and more. He is here today to talk about technical steps and measures you can take to prevent ransomware.



Here are the items we are going to cover in our presentation. We have a great mix of attendees today, so we are going to cover a few basics to start off with, and then get in to some technical items later in the presentation.


We have your City.
pay up, or else!
Ransom Note
How do ransomware extortionists gain access to business computers?
NHMA

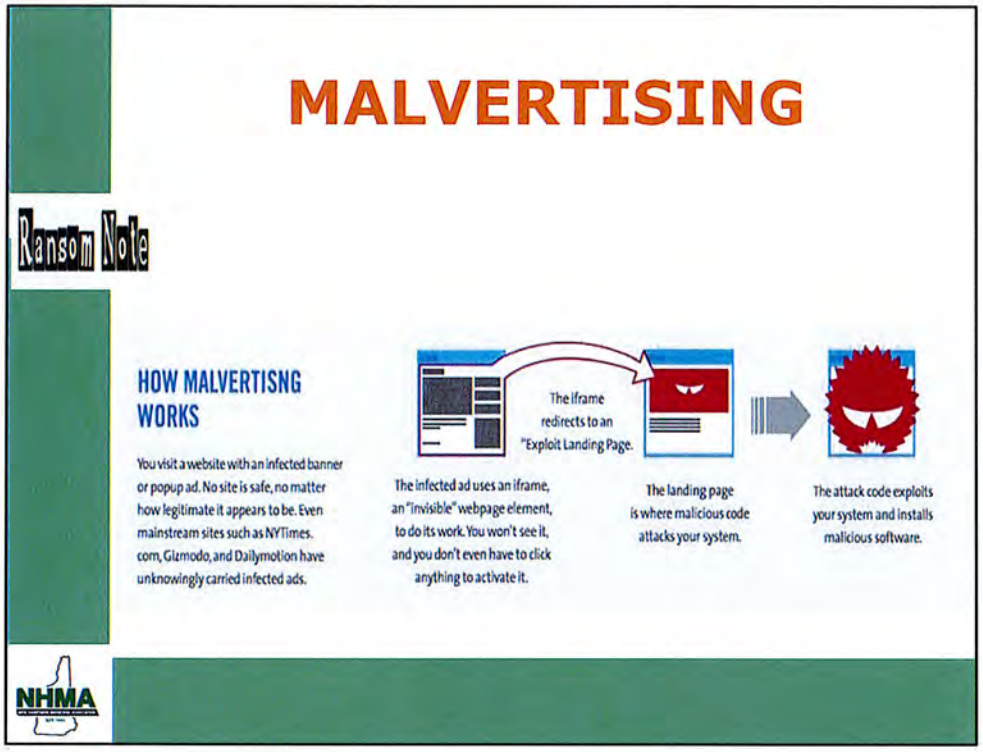
The unwanted commercial email – also known as "spam" – can be annoying. But worse, it can include bogus offers, or malicious links – and is a widely used to spread ransomware. Pictured here you see one of the most common scam emails .. This one is a "Brand Scam" and is especially popular in the holiday season. I think we take for granted that everyone is aware of these types of emails, but we really need to create more awareness in the workplace, and that is something we are going to get in to in the upcoming slides.



Spear phishing preys on the familiar. It is banking on the fact that the user is going to believe what they are seeing is legitimate. It can be from a familiar website, like that PayPal request you see above. It's also very popular to receive an email from a co-worker, or boss requesting access to something, or money to be transferred. All this information is really easy to gather on social media. In fact, I can go to LinkedIn right now, look up a company, and find out who the accounting manager and president are within about 1 minute. The information is already out there, and readily available to the hackers. You see, hacking is just as much about people, as it is about code. Phishing attacks According to the FTC, 93 % of all spear phishing emails contain a ransomware virus.

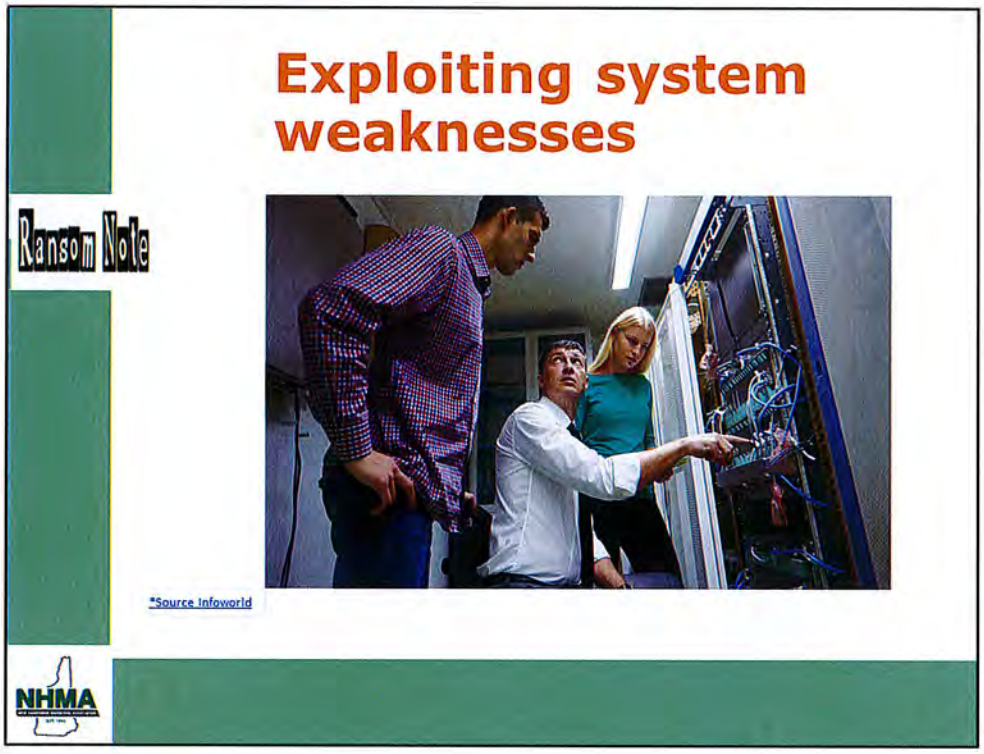
Greenland, NH received and email posing as AT&T and had a voicemail for the employee. Another town received an email that appeared as though it was from virtual town hall websites. Opened the attachment, and the PC was infected!

These criminals just keep getting smarter – How did they know to pose as a company frequently used by towns?



The cyber criminal is banking on the fact that you feel safe on a Trusted Companies website. BUT.. Any website can be infected by Malware.
Roughly 90,000 people a day are redirected from malvertising to a single proxy server. 10% of those, or 9,000 are vulnerable to an exploit (system vulnerability), of that 40% were compromised.

$34 million dollar per year



Ransomware attackers are no longer limited to drive-by downloads, preying end-users to inadvertently click on the wrong link.

SamSam ransomware is a new and improved string of ransomware. Designed to get a foothold inside the organization by exploiting known server vulnerabilities. Server vulnerabilities, exist in outdated systems, unmanaged systems.

The fact that SamSam targets servers makes it easier for the ransomware to cripple an entire department or organization, as the data on the servers are mission-critical to running a business. It's so much more than the users PC.

While SamSam ransomware is the most immediate threat targeting web based servers, it isn't the only attack to worry about. Nothing is preventing attackers from using a compromised server to then launch denial-of-service

attacks or consume resources to mine bitcoins, for example.

We cannot stress enough the importance of patching software regularly and on time. Patching is critical but frequently neglected -- by organizations and by the software vendors themselves. Some of the SamSam attacks exploited weaknesses that should have been patches 7 to 9 years ago! According to a scan by cisco there are approximately 3.5 million vulnerable machines out there.

***Not keeping up with security patching can have a devastating impact on an organization.

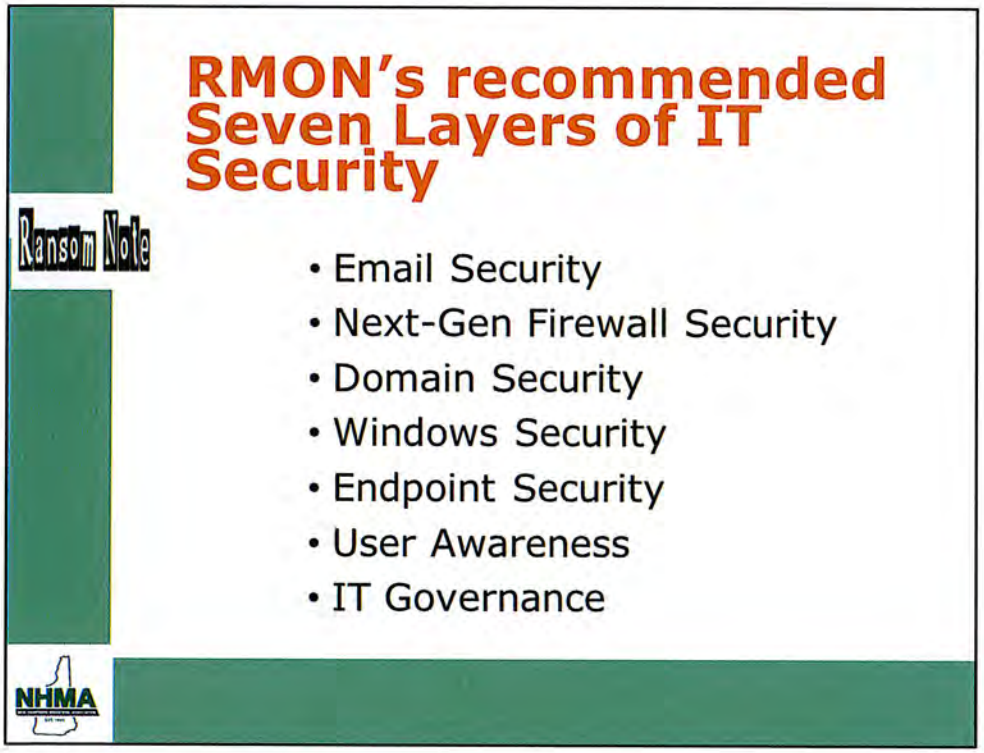
How to reduce your business risk and suggested technical implementations

Ransom Note

Normal Glass

Bullet proof glass consisting of normal glass (blue) and polycarbonate (red) layers

NHMA



What is "Network Hygiene". Good network hygiene is really about keeping your network up to date and clean. Knowing your inventory, users, devices that are connecting, where your data can end up. It's really understanding what you have going on in your computer network.

According to the Online Trust Alliance, 90% of all ransomware attacks could have been prevented with good network hygiene.

With that being said, you really need to focus on hygiene and prevention, because once you are hit, it's pretty much impossible to get your data back. With that being said... You need to have a backup.

Email Security

Ransom Note

- Spam filter
- Email link scanning
- Extension blocking

NHMA

Next-Gen Firewall Security

Ransom Note

- IPS/IDS
- Web Filtering
- Download and Email Scanning
- Blacklisting
- Access Controls

NHMA

Domain Security

Ransom Note

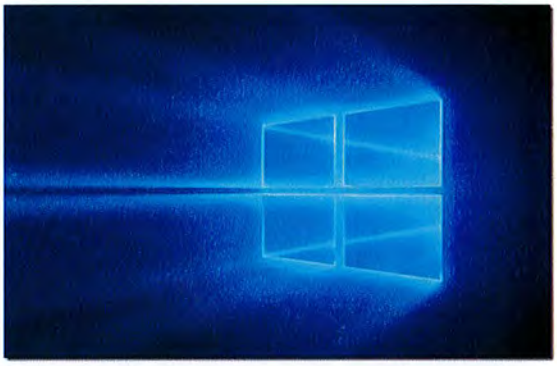
- Complex Password Policies
- Software Restriction Policies
- Share and File Security
- Disable Default Accounts
- Domain Auditing

NHMA

Windows Security

Ransom Note

- Windows Patching
- Port Hardening
- Disable Windows Scripting Host/VBS scripts
- Limit Domain/Local Admins
- Show hidden file extensions
- Modern Browsers



NHMA

Endpoint Security

- Antivirus and Anti Malware
- Sandboxing and Host Intrusion Prevention Systems
- Browser Plug In Patching
- Disable Autorun on drives
- Disable Autoplay in browsers
- Enable Addblocking
- MDM

NHMA

Governance

Ransom Note

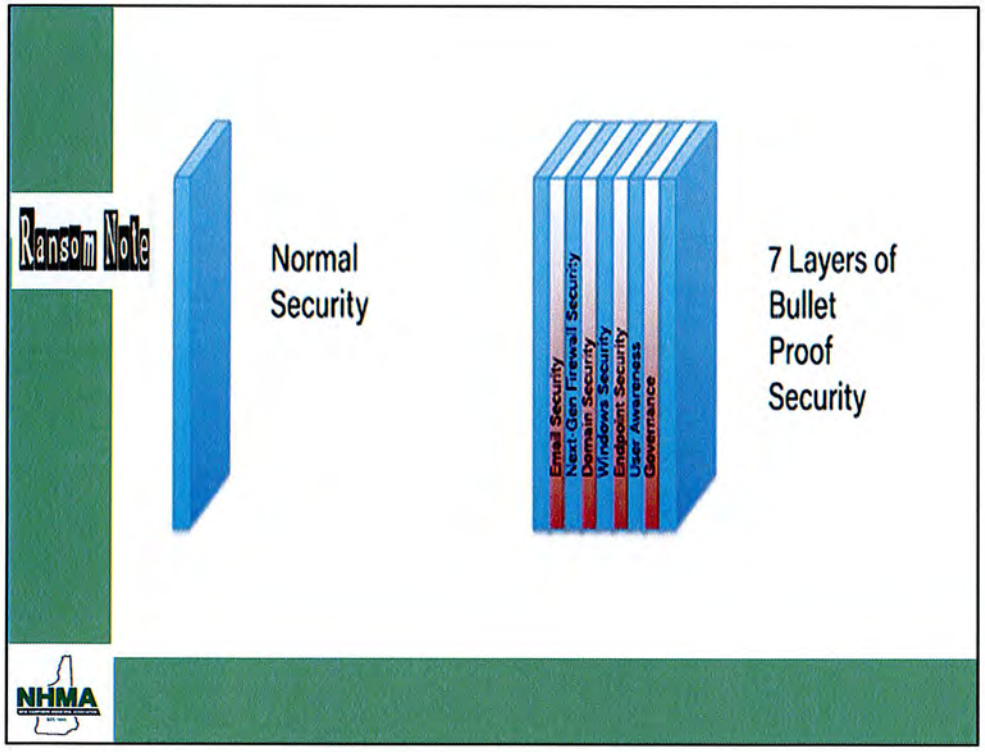
- Monitoring
- WISP
- BC/DR Planning

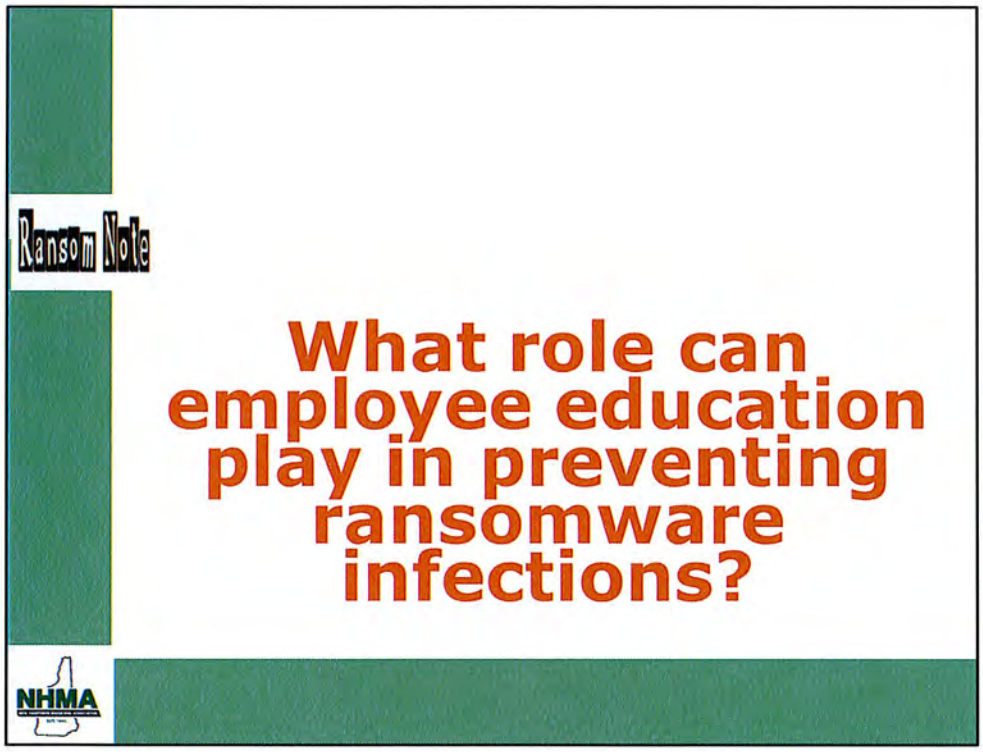
User Awareness

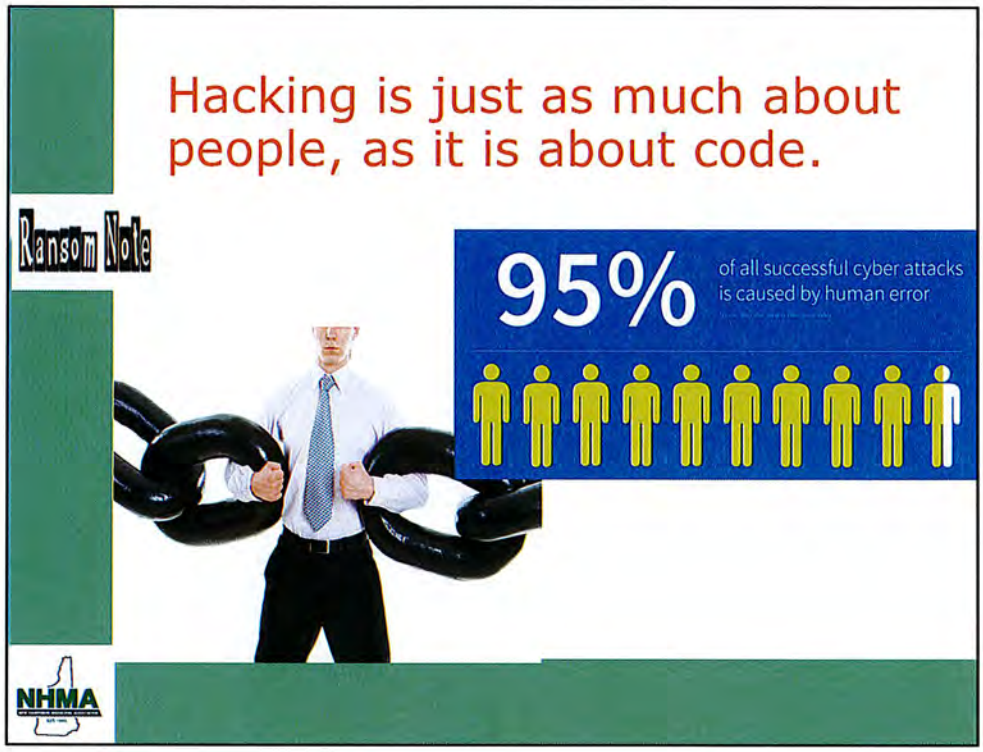
Ransom Note

- Malvertising and Phishing Education
- Device security and usage training

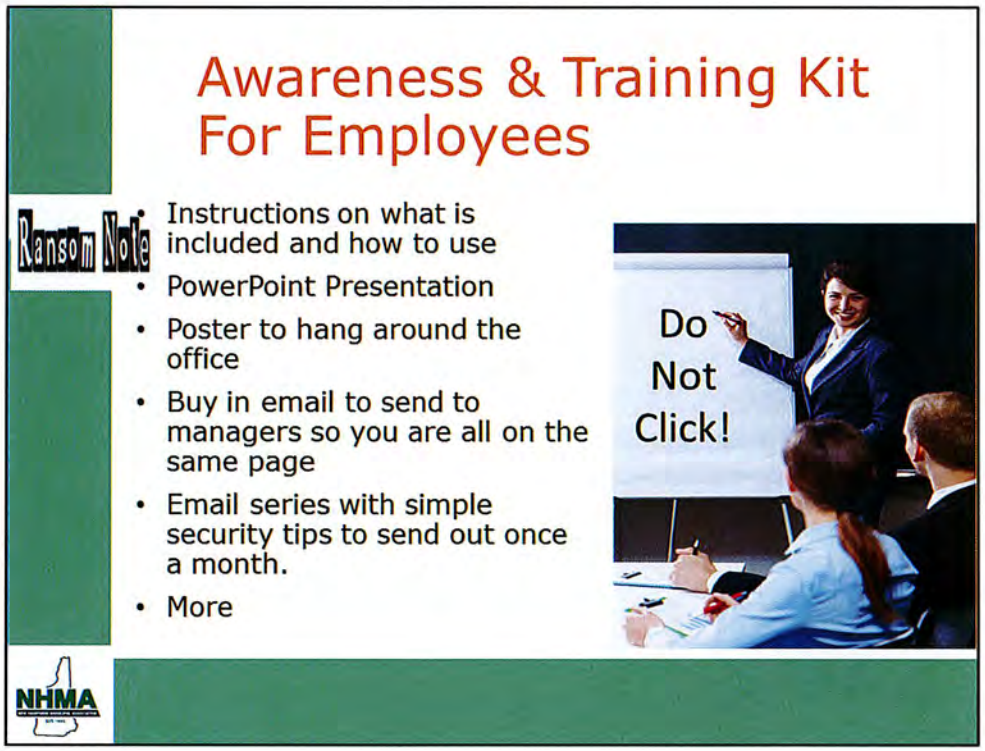
NHMA


Ransom Note
Normal Security
Email Security
Next-Gen Firewall Security
Domain Security
Windows Security
Endpoint Security
User Awareness
Governance
7 Layers of Bullet Proof Security
NHMA

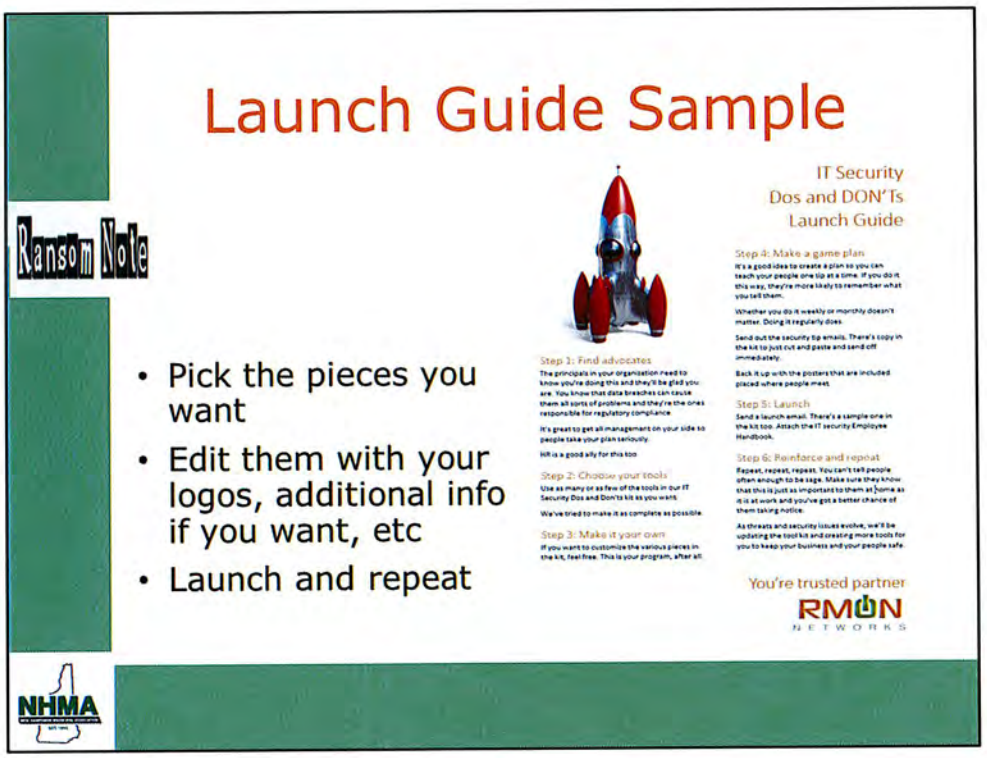

Ransom Note
What role can employee education play in preventing ransomware infections?
NHMA



As I stated earlier "hacking is just as much about people, as it is about code". We cannot stress enough promoting employee education & simple awareness programs. We all assume people know when something is a scam… but if that were true hackers would not be as successful as they are.

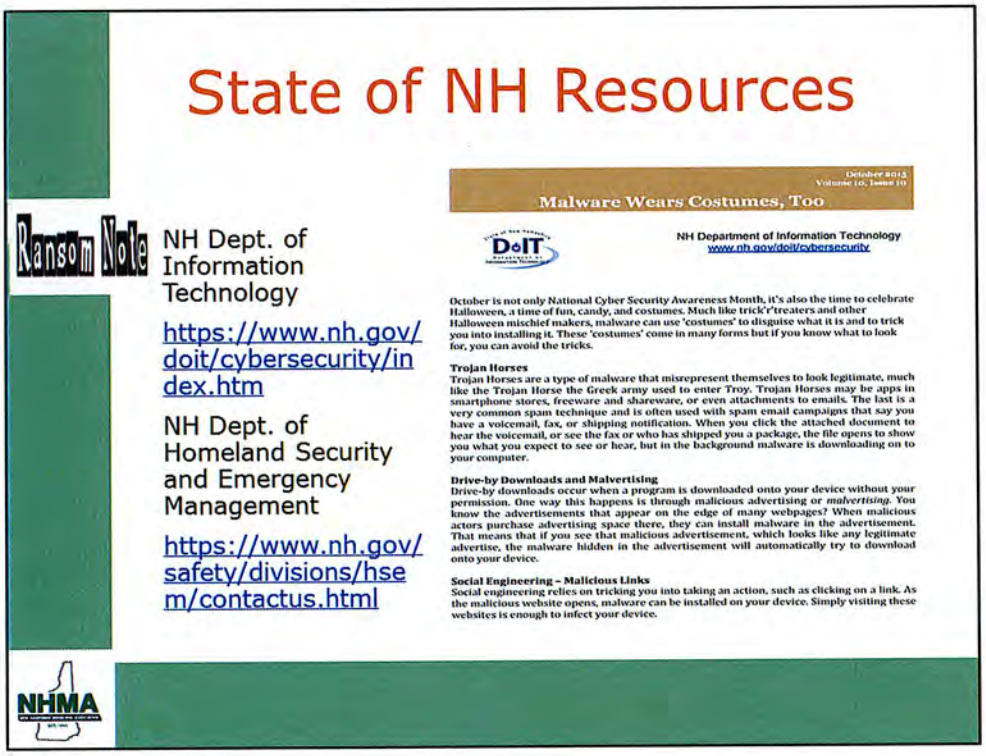


We have been providing a great user training kit for FREE on our website for quite a few years now. It is completely editable, so you can brand it yourself. It has everything you need to start an awareness program in your office.



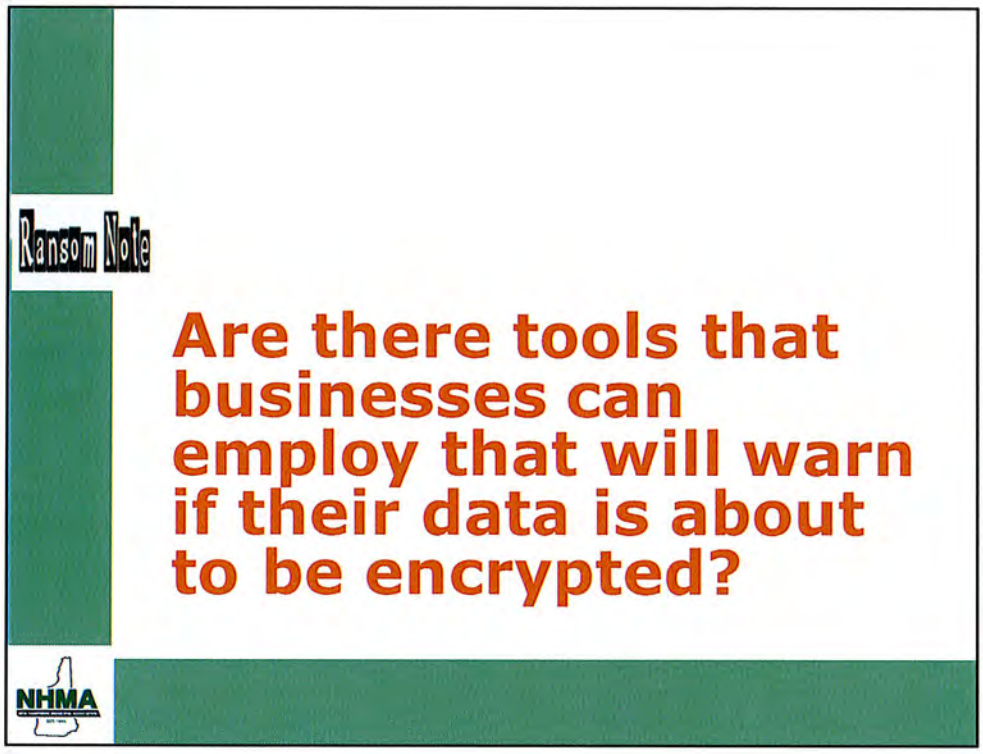
We have some samples here of what is in our training kit. You can use this as a starting point. Change, or add what ever you'd like.

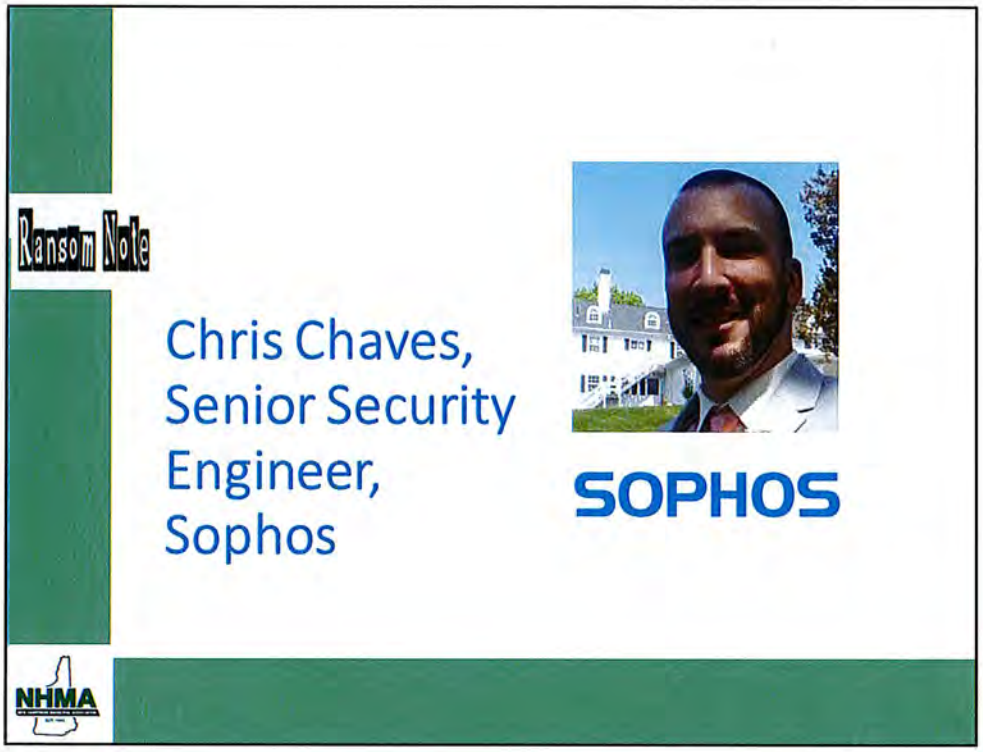
We have some samples here of what is in our training kit. You can use this as a starting point. Change, or add what ever you'd like.



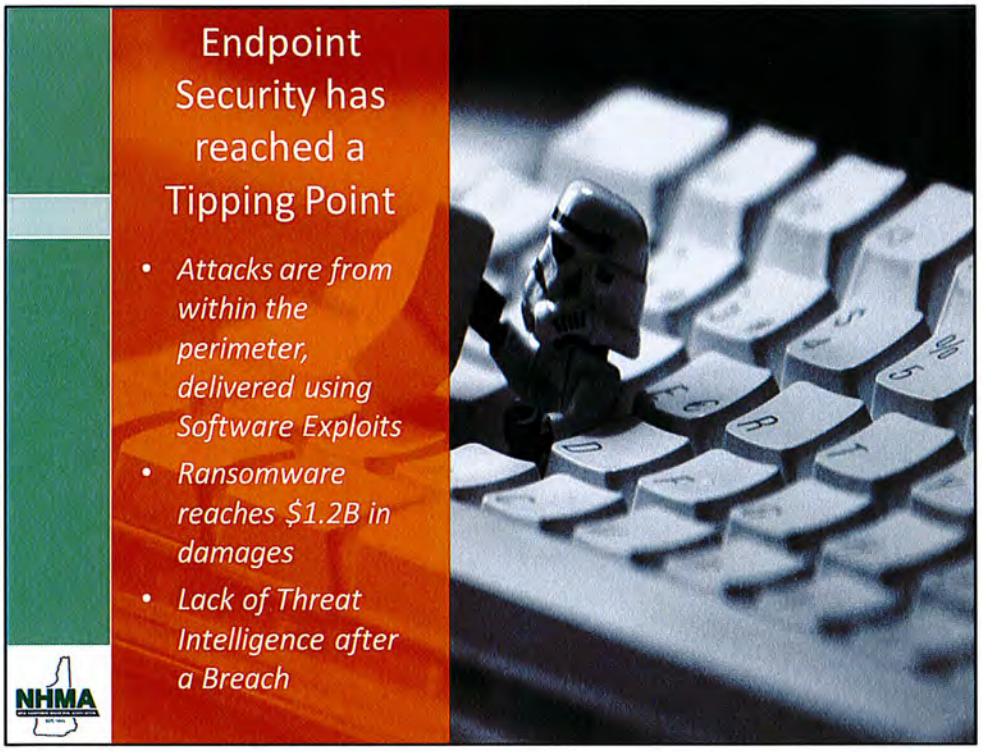
The NH Department of Information Technology has great information that you can share with employees for awareness training! These would be great article to share once or twice a month!

FTC is another great resource for information as well. These will all help you build programs.


Ransom Note
Are there tools that businesses can employ that will warn if their data is about to be encrypted?
NHMA



Thank you David. And now we are going to turn over the presentation to Chris Chaves from Sophos. Sophos is a leader in the security industry, and one of our trusted partners. Chris is here to discuss their revolutionary new product called Intercept X. We just discussed a key component to preventing ransomware is utilizing all of the features your endpoint has available. InterceptX is additional layer for Endpoint Security, and it was just released mid – September, and it can actually STOP ransomware! This is really exciting, I think the technical folks on the line will really appreciate this portion of the presentation. Welcome Chris Chaves.



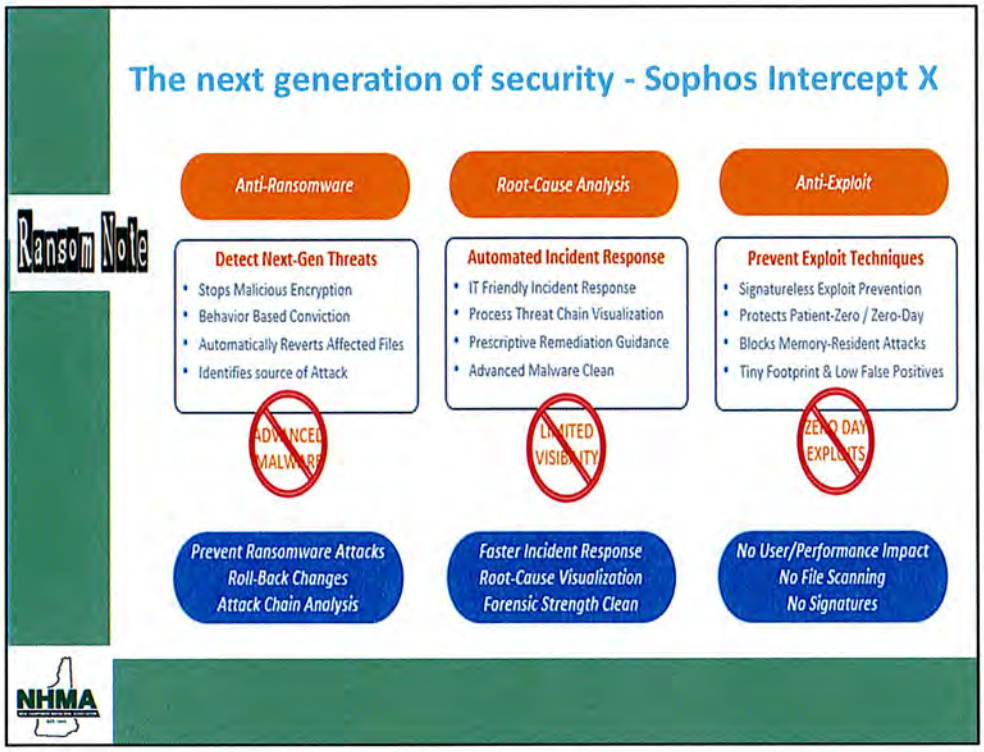
Setting the scene – why do we need InterceptX

Attacks are focused on the endpoint, evading traditional perimeter defenses, using software exploits to deliver malicious payloads

90 % of breaches are from software exploits – NSS Labs

90+ % of exploits are from known vulnerabilities – ie: non zero day, patches available

66 % of IT staff lack incident response skills (Sans Survey into Incident Response)



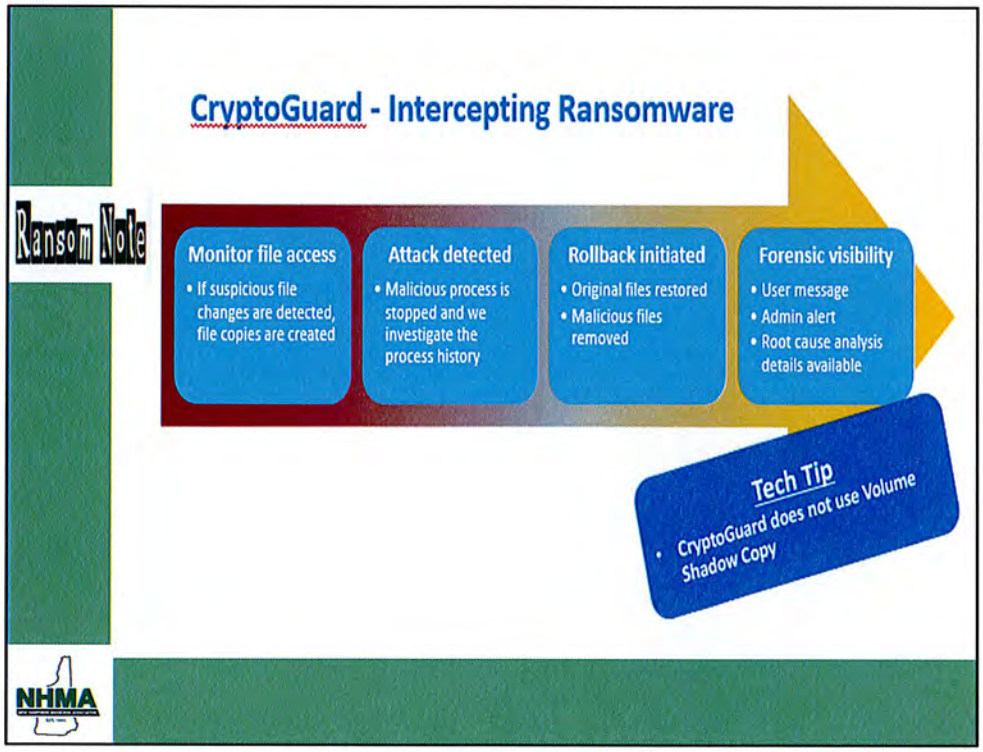
The existence of advance malware such as crypto-ransomware variants presents a very visible problem.

Yet IT and security teams have limited visibility in to the threats hitting their endpoints today.

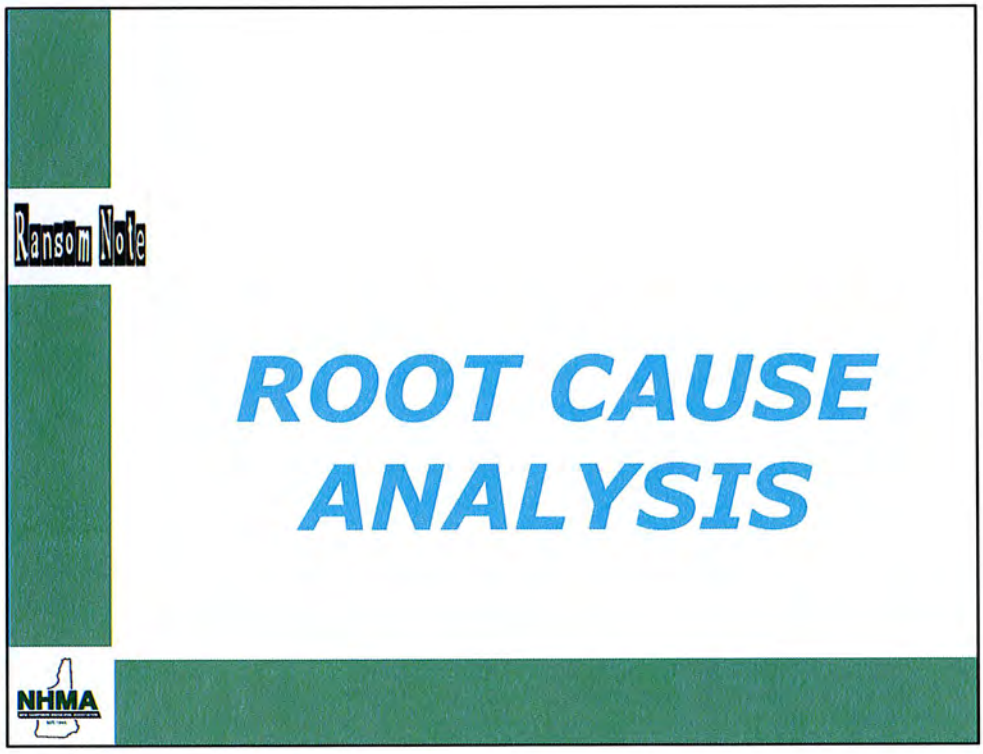
And the software we use daily is being turned against us – the number of software vulnerabilities being recorded is increasing, we have to patch and patch fast – but patching is like closing the stable door after the horse has bolted.

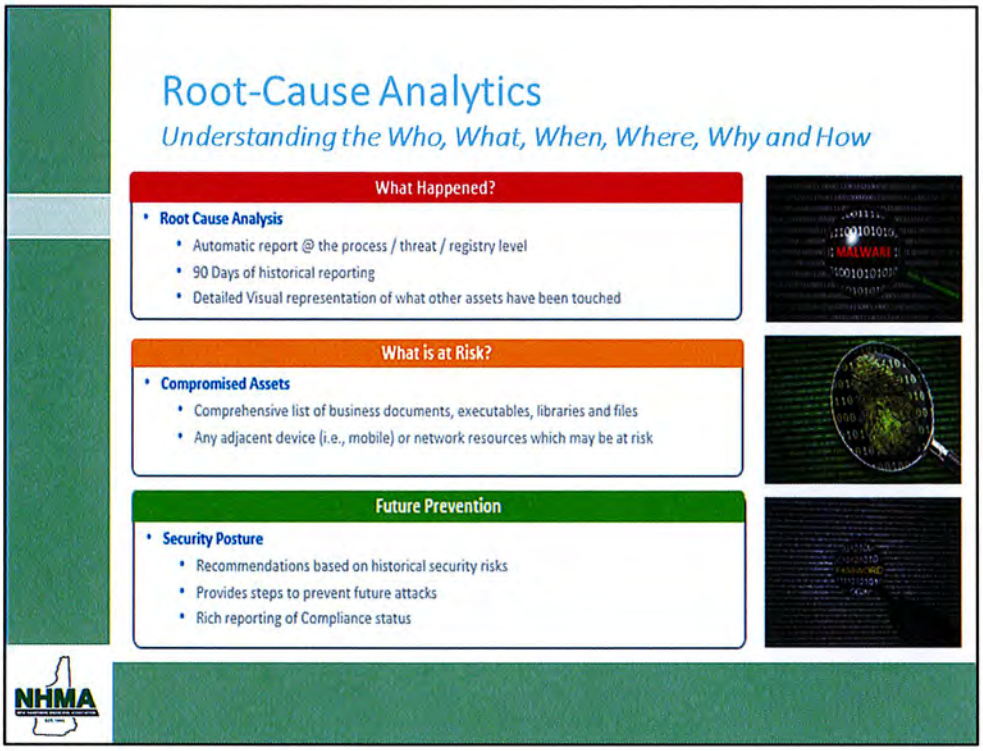
Enter the next-generation – a completely new approach to endpoint security


Ransom Note
ANTI-RANSOMWARE
NHMA

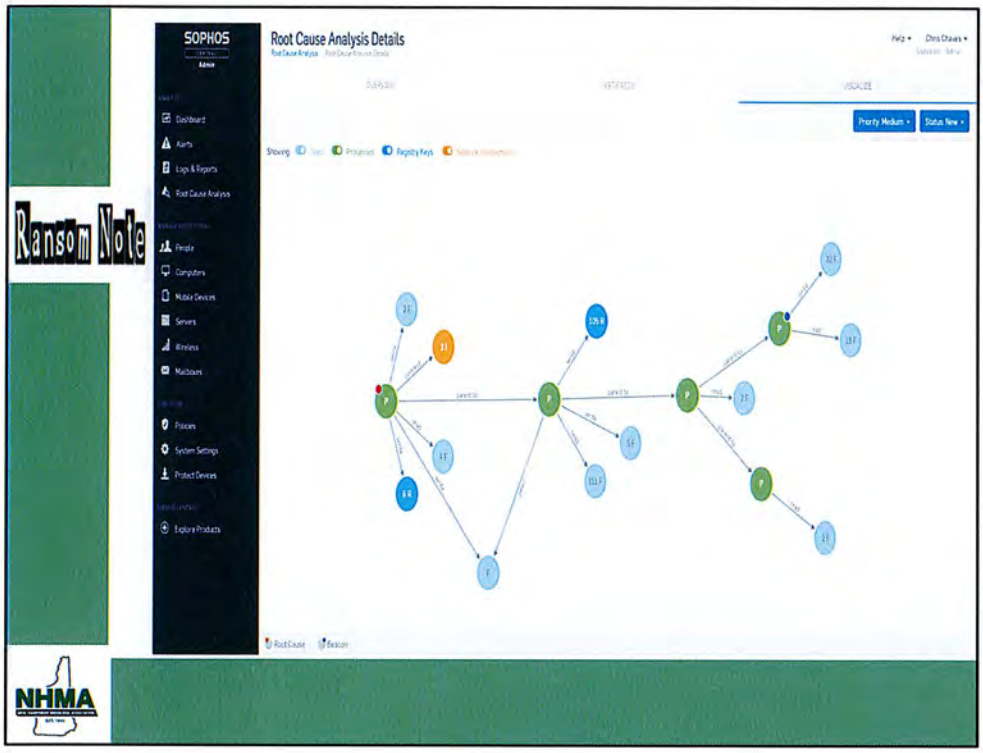


Monitor for distinct changes in the file headers

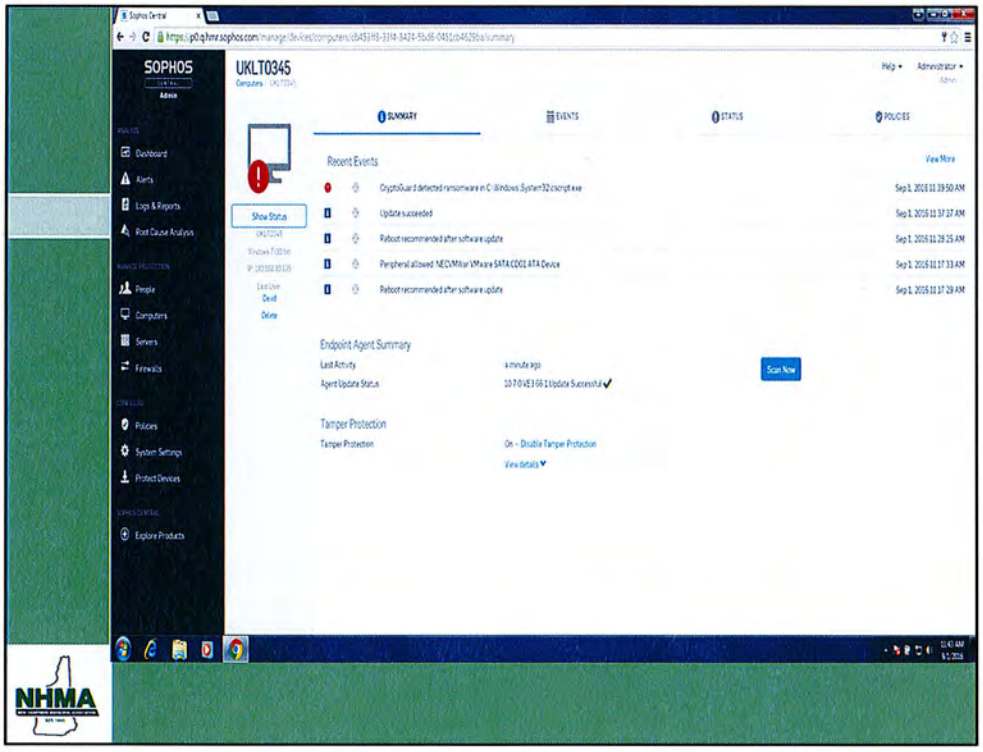

Ransom Note
ROOT CAUSE
ANALYSIS
NHMA



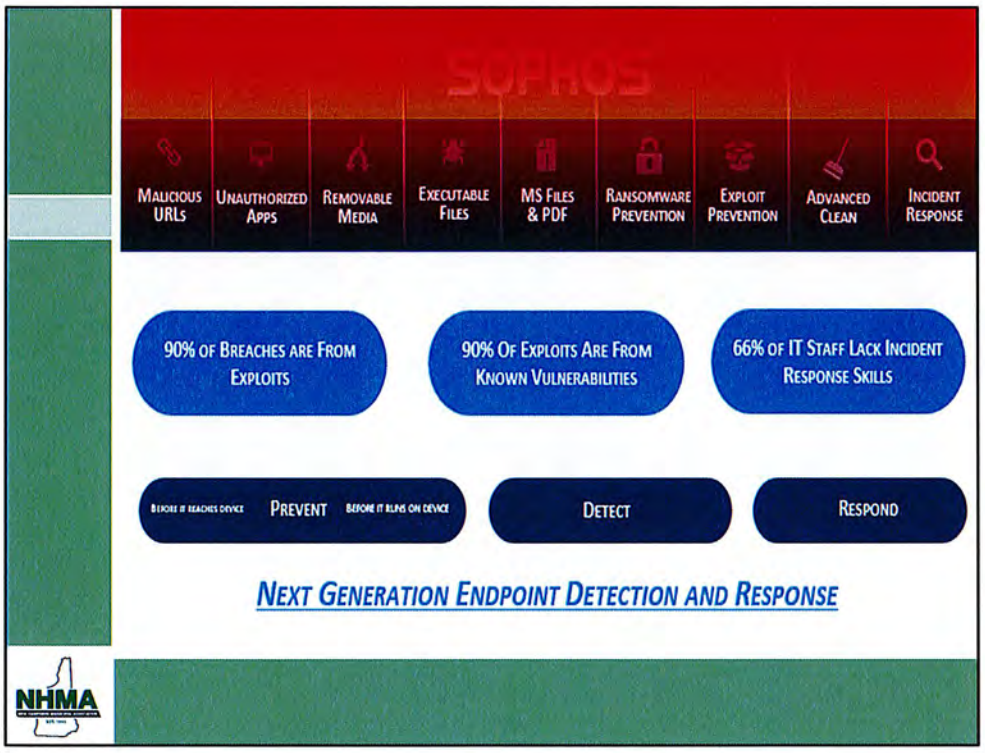
Monitor for distinct changes in the file headers



Our Incident Response engine automatically capture core data on an incident. Showing crisp summary data and details a human can understand. PLUS IT people can add comments and actions to each incident as its investigated. We AUTOMATICALLY add a priority depending on our analysis of the root cause and the chain itself. Obviously someone can add to this, for example here is a piece of ransomware attempting to start encrypting your business files.

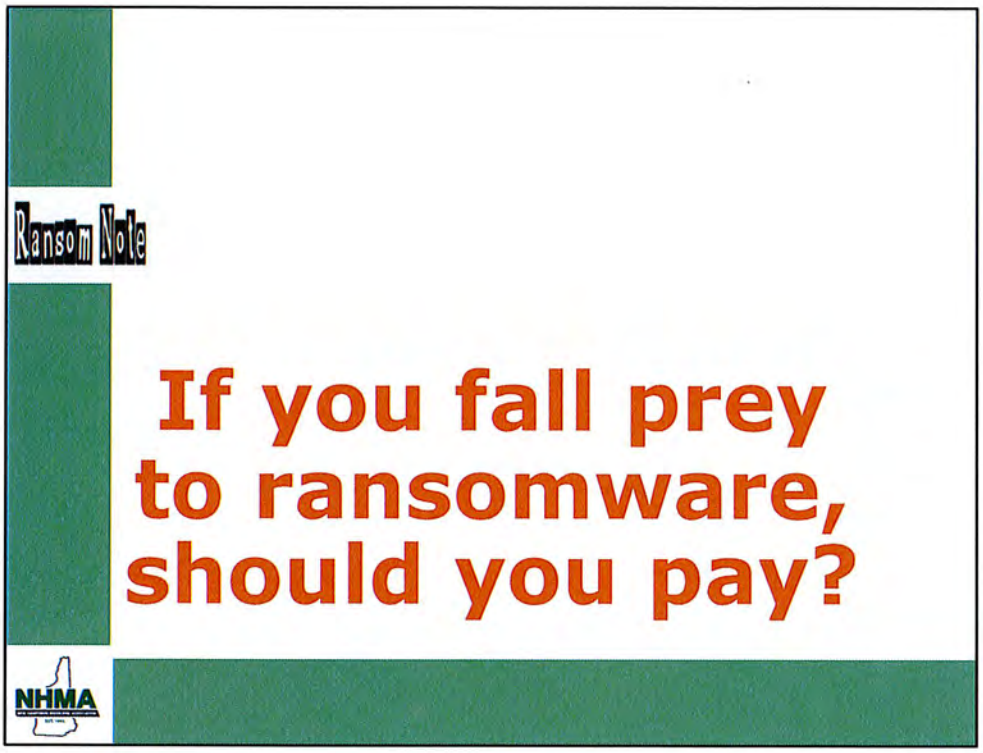

SOPHOS
Admin
Dashboard
Alerts
Logs & Reports
Root Cause Analysis
People
Computers
Servers
Firewalls
Policies
System Settings
Protect Devices
Explore Products
UKLT0345
Help
Administrator
SUMMARY
EVENTS
STATUS
POLICIES
Show Status
Recent Events
View More
Update succeeded
Reboot recommended after software update
Peripheral allowed: NECVMWar VMware SATA CD01 ATA Device
Reboot recommended after software update
Endpoint Agent Summary
Last Activity
Agent Update Status
Scan Now
Tamper Protection
Tamper Protection
On - Disable Tamper Protection
View details
NHMA

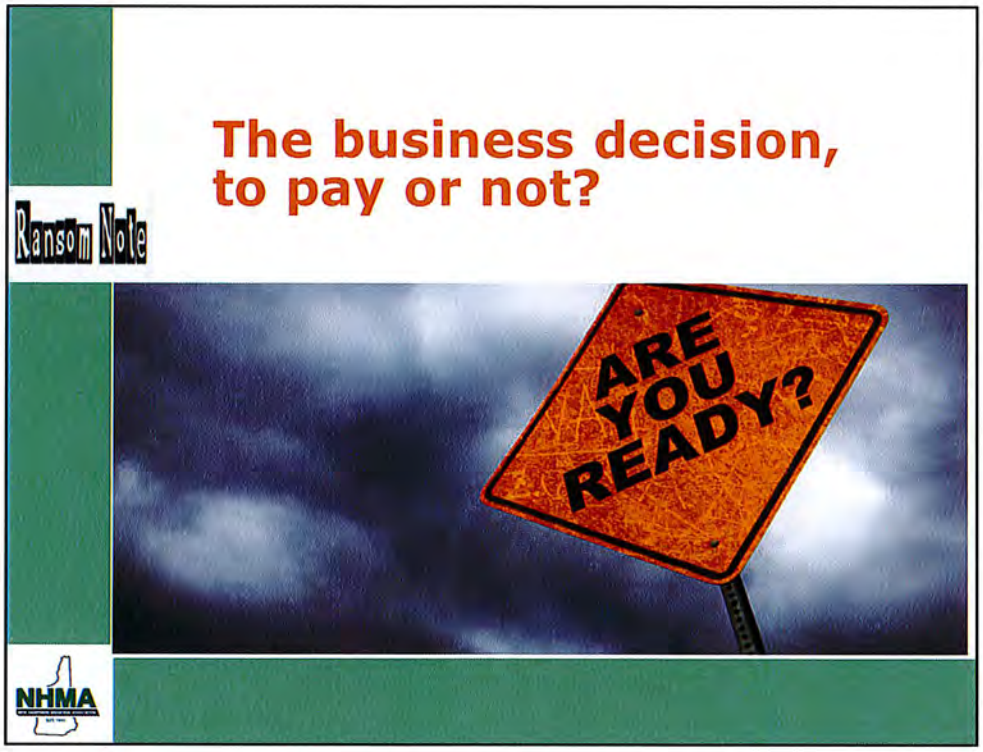
Most popular exploit payload – Ransomware.



Only by adding Intercept X on top of Endpoint Advanced do you truly build, complete next generation endpoint detection and response capabilities.

You can choose to build your own by layering intercept x on top of their chosen endpoint – adding anti-exploit, anti-ransomware and greater visibility to your current suite.


Ransom Note
If you fall prey to ransomware, should you pay?
NHMA

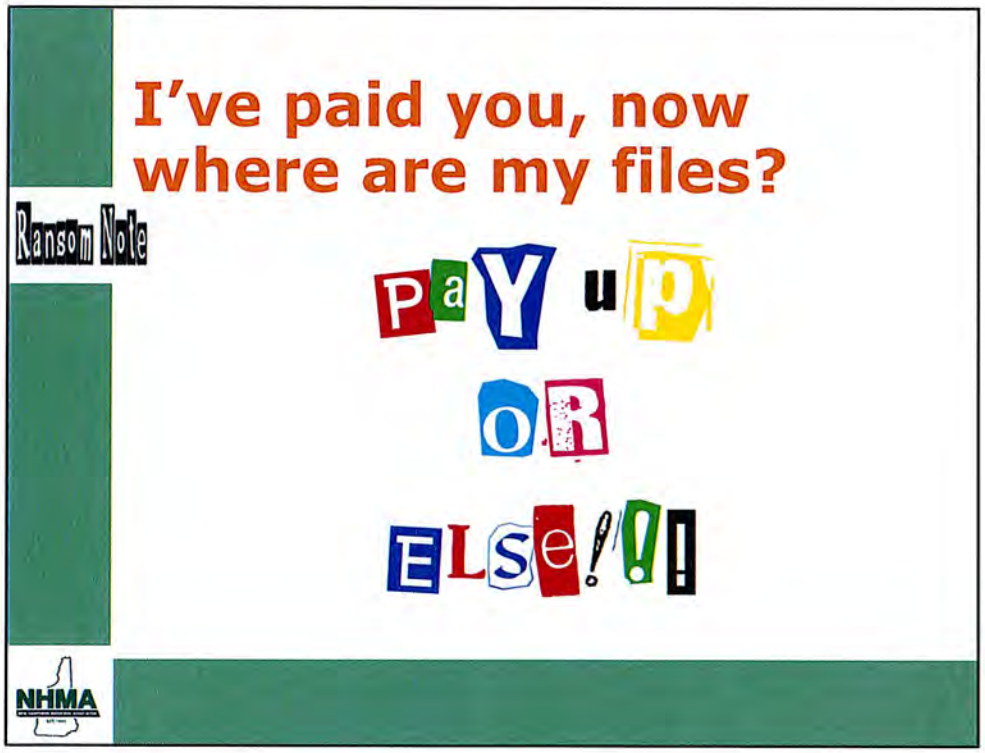


This is a business question is totally up to you. Obviously you do not want to have to pay and encourage the bad guys. Sometimes people have to. There are a lot of unreported cases because people are embarrassed. If you work at a company you should absolutely tell your IT Department because they hopefully have a backup.

There is going to come a day when this will become more than about money. Criminals may someday ask you to steal confidential business data.

With the internet of thing just consider what the future of ransomware could be. Need to get to work? Pay me, or I won't start your car. It's freezing outside, don't want your pipes to freeze, pay me or you won't have access to your thermostat controller.

So, be prepared, and don't pay if you don't have to.

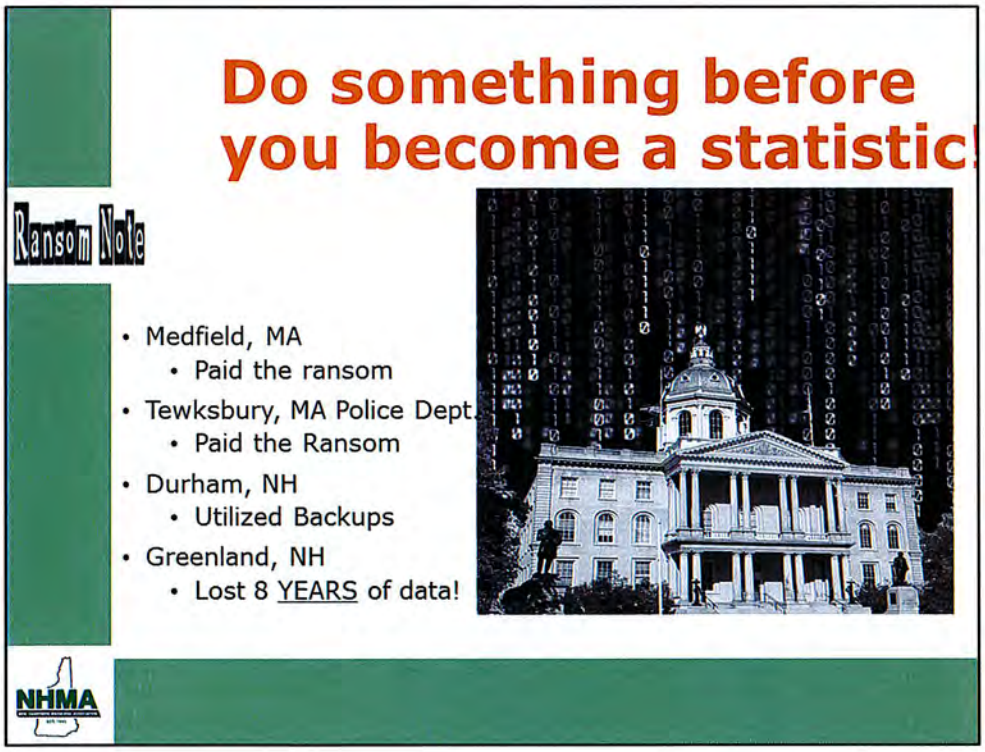


Ransomware has built a trustworthy reputation for itself. Victims have paid the ransom, and then they get their files back.
However, if you have a bit of experience with ransomware, then you know this is not always true.

- Something could go wrong in the decryption process.
- The hacker could decide he wants more money.
- Your files could get re-encypted all over again, if you don't properly remove the virus.

In the case of Greenland, NH the information did not make it to the town administrator in time, and it was just too late!
The point is… Cyber criminals really cannot be trusted, despite the image they have created.

We really hope it never has to come to this point for you. That is why we are here today educating you on the prevention methods for not only your systems, but users too.



This information is only what is in the Media! Trust me, there are many other stories that are not being reported. There are stories from towns we have spoken with each year at the annual conference that were nearly as bad as the Greenland!

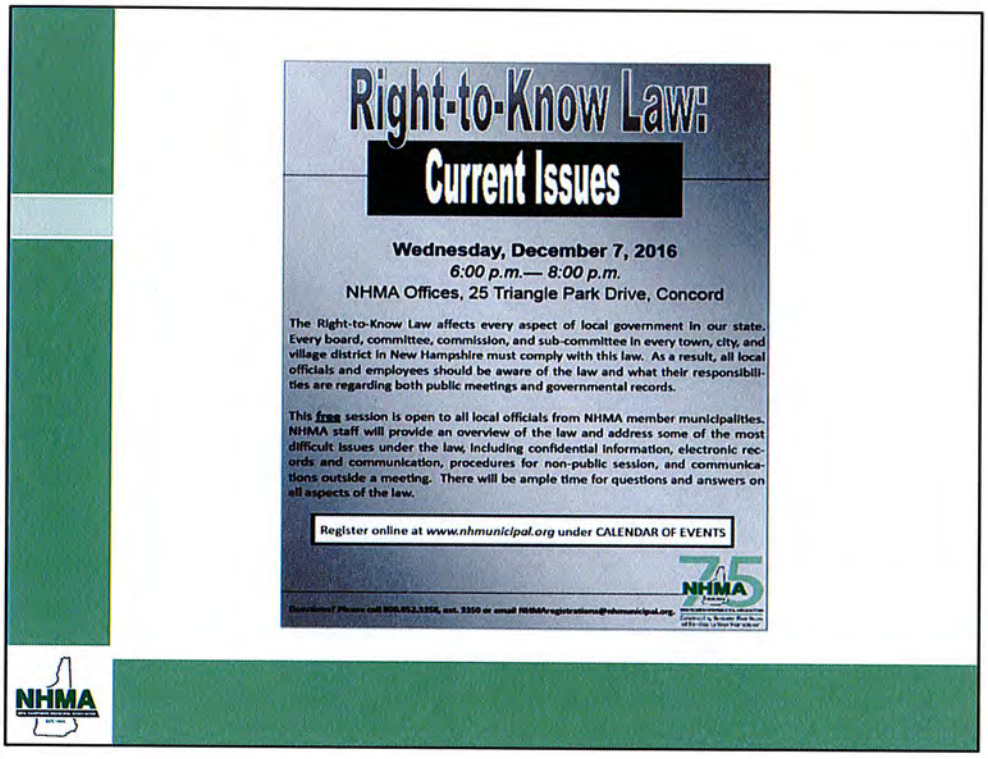
When you think about the type of information that state and local agencies hold, like resident's tax information, property information, social security numbers, birth and death certificates and emergency contact information, we really hope that people don't have to learn the hard way when it comes to ransomware.

This information is only what is in the Media! Trust me, there are many other stories that are not being reported. There are stories from towns we have spoken with each year at the annual conference that were nearly as bad as the Greenland!

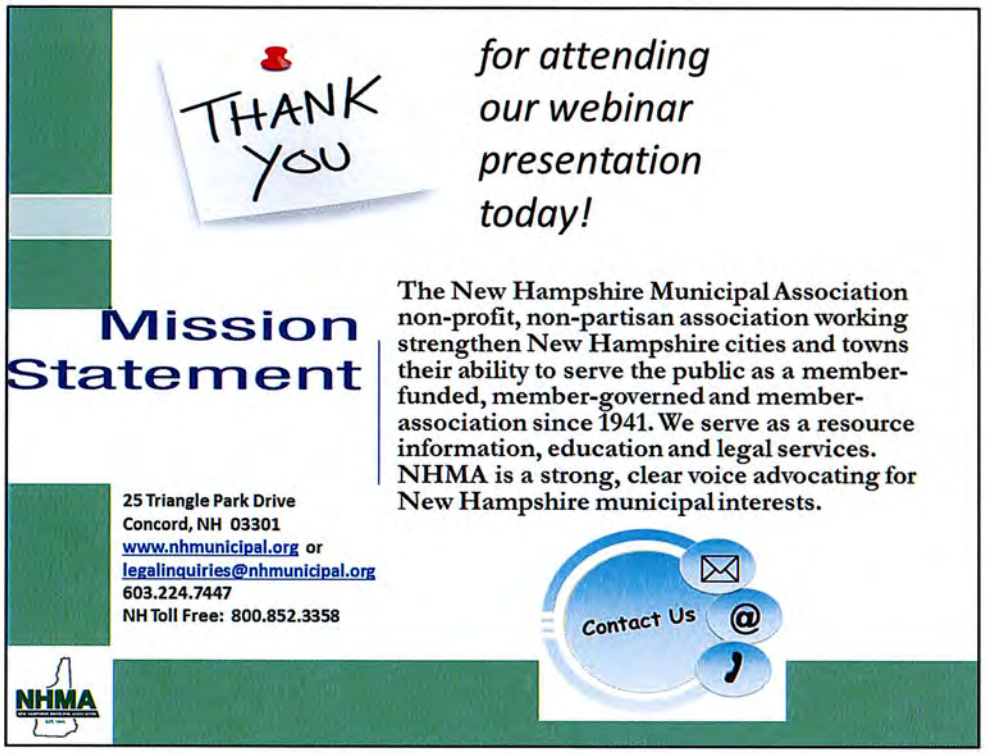
When you think about the type of information that state and local agencies hold, like resident's tax information, property information, social security numbers, birth and death certificates and emergency contact information, we really hope that people don't have to learn the hard way when it comes to ransomware.


PROD.
COMING ATTRACTIONS
November 7
Asset Management Time Machine
VENUE
www.nhmunicipal.org
NHMA


PROD.
COMING ATTRACTIONS
December 7
Exploring Infrastructure
Funding Strategies
VENUE
www.nhmunicipal.org
NHMA


Right-to-Know Law:
Current Issues
Wednesday, December 7, 2016
6:00 p.m.— 8:00 p.m.
NHMA Offices, 25 Triangle Park Drive, Concord
The Right-to-Know Law affects every aspect of local government in our state. Every board, committee, commission, and sub-committee in every town, city, and village district in New Hampshire must comply with this law. As a result, all local officials and employees should be aware of the law and what their responsibilities are regarding both public meetings and governmental records.
This free session is open to all local officials from NHMA member municipalities. NHMA staff will provide an overview of the law and address some of the most difficult issues under the law, including confidential information, electronic records and communication, procedures for non-public session, and communications outside a meeting. There will be ample time for questions and answers on all aspects of the law.
Register online at www.nhmunicipal.org under CALENDAR OF EVENTS
NHMA
75
NHMA

Visit NHMA's Anniversary Webpage: www.nhmunicipal.org/anniversary


THANK YOU
for attending our webinar presentation today!
Mission Statement
The New Hampshire Municipal Association non-profit, non-partisan association working strengthen New Hampshire cities and towns their ability to serve the public as a member-funded, member-governed and member-association since 1941. We serve as a resource information, education and legal services. NHMA is a strong, clear voice advocating for New Hampshire municipal interests.
25 Triangle Park Drive
Concord, NH 03301
www.nhmunicipal.org or
legalinquiries@nhmunicipal.org
603.224.7447
NH Toll Free: 800.852.3358
Contact Us
NHMA