Lessons learned from a Ransomware Attack

Hi my name is Ski. My coauthor is Jon Biggerstaff. This talk will cover a ransomware attack at the Northshore School District in the fall of 2019. I will talk briefly about our environment, then cover the attack, before spending most of the talk on the lessons we learned.

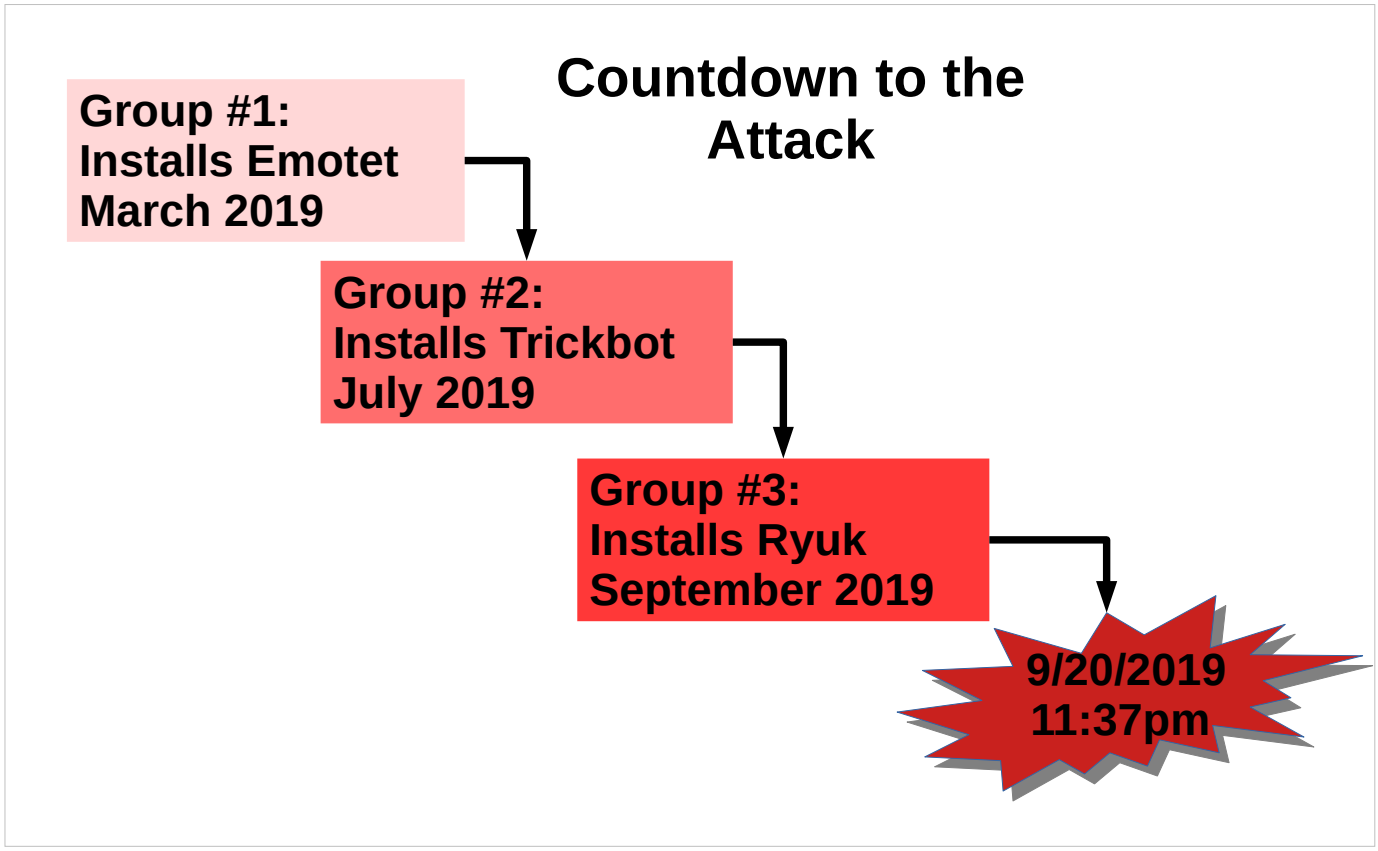
-

We were very surprised by the attack. We had spent years assuming that school districts were not really targets since we don't have customer accounts or credit card information. We knew we needed to improve our security but couldn't get it identified as a district priority.

-

However, school districts are good targets for ransomware because they have small technical staff and large budgets. In 2019, over 1,000 schools were hit by ransomware, some of them multiple times!

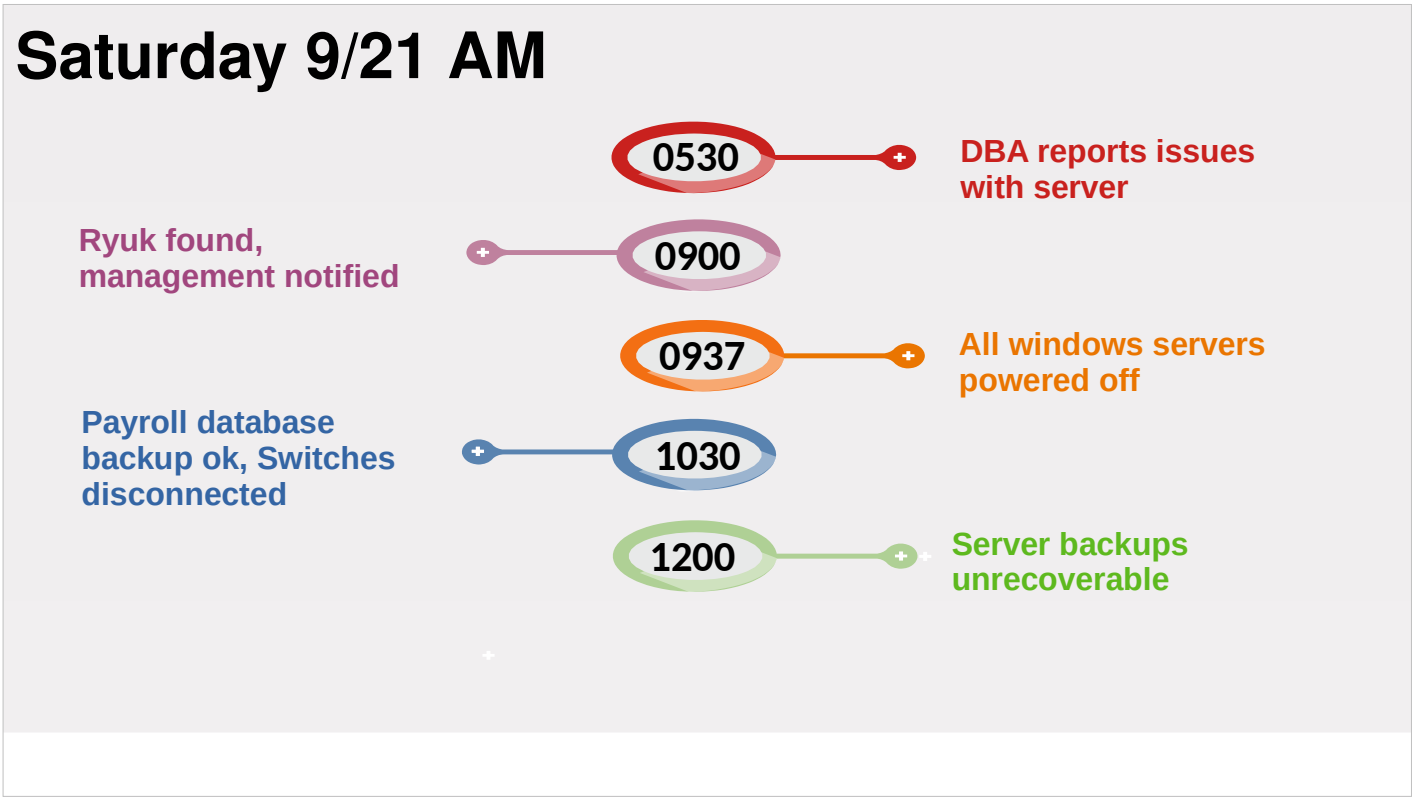
Northshore is a mid-sized school district with 4000 staff and 23000 students spread over 38 sites and 60 sq miles. The datacenter consisted of 300 windows, linux, and blackbox servers running on VMware with a 400TB mix of NAS and iSCSI storage. Client devices include a mix of windows, mac, chromebook workstations, and iPads. We are a 5x10 shop and, like most school districts, severely understaffed for the workload. Security was never made a priority by our administration because it is more costly, requires more staff, and is usually inconvenient. At that time, we were told that our most critical services (other than core network services) were the Student Information System, Payroll, Phones, and Email.



We were required to report the event to the FBI who also brought in Homeland Security. They told us about the organizations behind our attack. First the Emotet group infected our systems and offered us up for bid once enough computers were infected. The group that won the bid deployed Trickbot to get admin level permissions for key systems. Once the second group had admin permissions, we were offered up for bid a second time which a RYUK group won. The RYUK groups are even more interesting because the original developers of RYUK operate like a franchise, licensing the code and getting payments in return for successful attacks.

-

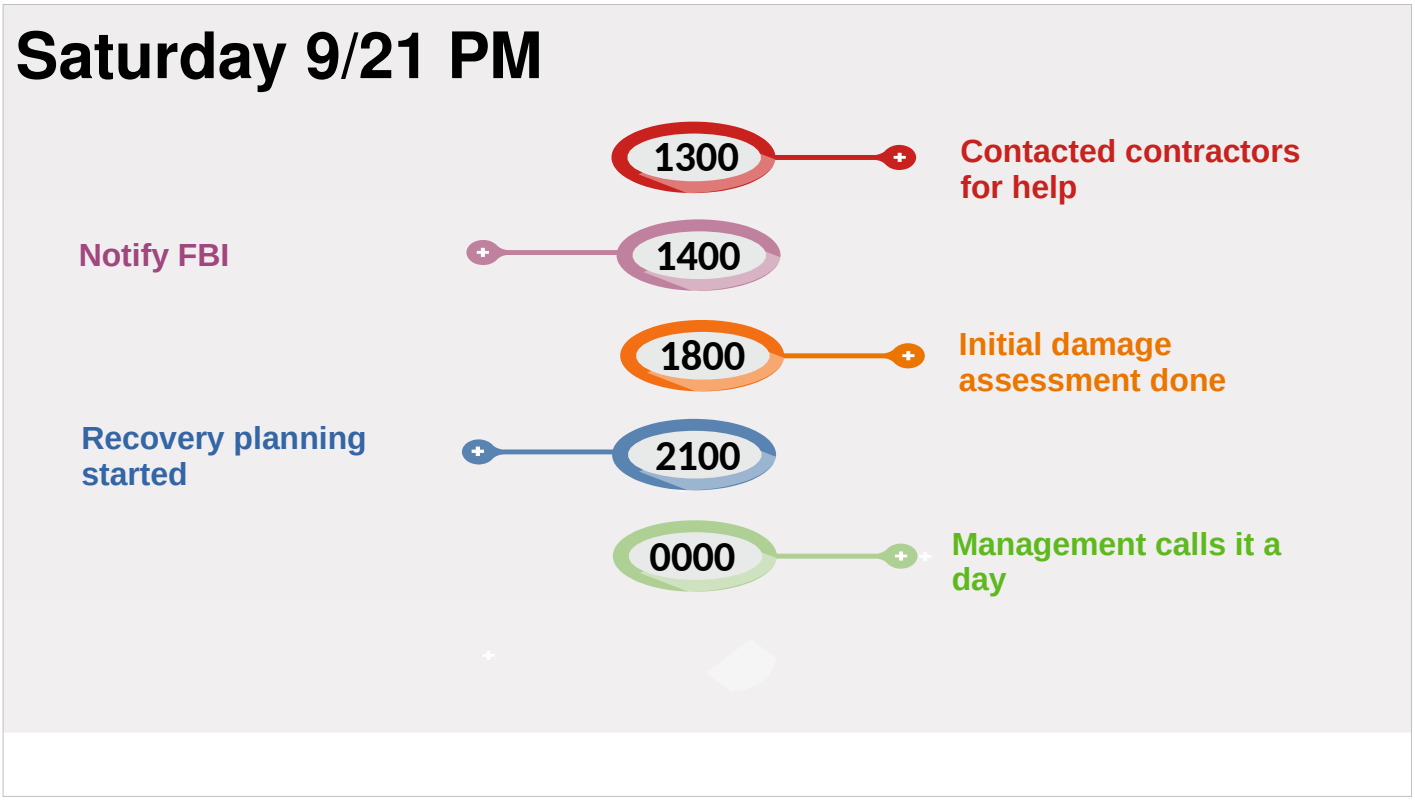
Attacks are typically triggered on late Fri or early Sat to minimize detection, and right before a major process such as payroll to maximize pressure on their target to pay. The attack on our systems began at 11:37pm on Friday September 20th. Our payroll was scheduled to run in 4 days on September 24th. Note that the events leading up to the attack take place over months - not weeks or days.



A ransomware attack is an emotional rollercoaster. When you are first hit, you are not be looking for ransomware, but instead for a reason why a server is not working correctly. There is panic once the issue is identified as ransomware and the extent of the damage is discovered. There is hope at various times while you check systems and backups thinking you had measures in place to keep this from spreading or to protect backups, but then despair when you find that the measures didn't work. This is even worse for those you report to who don't understand the technical issues and may not understand why the report keeps changing as you investigate more systems.

-

The despair we felt when we discovered that our backup server had been successfully hit as well and we would have to rebuild 180 windows servers and Active Directory from scratch I would not wish on anyone. The attackers corrupted both our local and AWS file systems where the backups were stored. In a perfect example of Murphy’s law, our AWS datastore which is normally disconnected and acted as an airgapped backup, was still connected this weekend because we were replicating backups to AWS.



Realizing we were going to need more help, we started contacting contractors and at that point notified the FBI. Each technology team focused on triaging their area to figure out the extent of the damage.

-

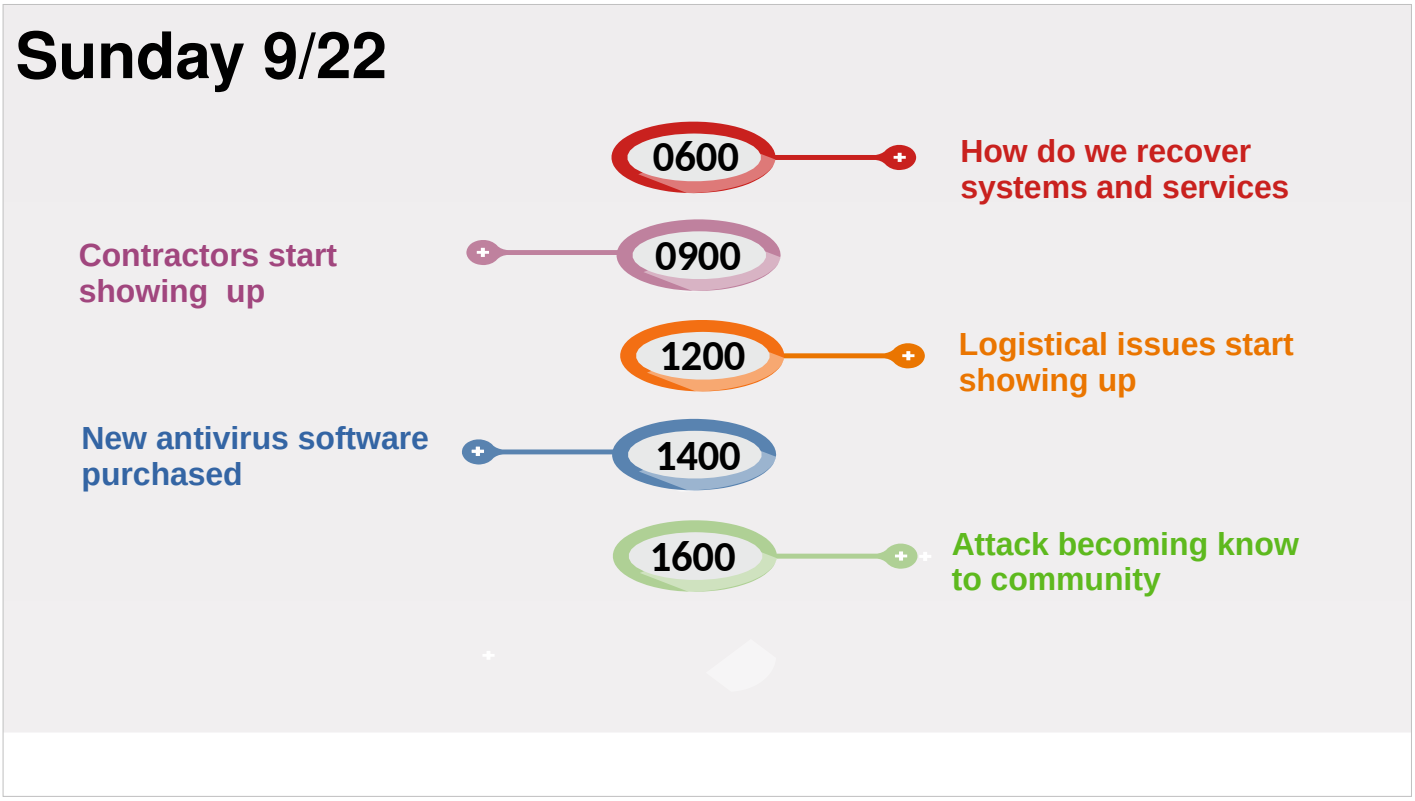
The good news was that all NAS data was recoverable due to snapshots and most database backups were stored on the NAS. In addition, all of our network services, email, and the classroom management service were running as they were either not based on Windows or are hosted. Most of our staff and students were not on windows workstations so most they were only minimally impacted.

-

By 9pm we were planning for how to recover the infrastructure and in what order. Active Directory was a top priority as that was used for authentication across many systems and impacted everyone. Payroll was also, as that is a major legal issue if it does not go out on time and the Student Information System as it is used by staff, students and parents daily. The phone system was just behind that as schools typically get hundreds of voicemails every day.

-

Our leadership sent us home at midnight to avoid burnout.



By day 2, we had identified the affected systems and likely available backup data and were working to get things fixed. Various teams worked on setting up a new Active Directory domain, building new virtual server templates, rebuilding the payroll system, reviewing network logs, and rebuilding the ESXi hosts as we are concerned with backdoors. New anti-malware software was purchased as our existing software did not detect anything.

-

We started to run into management and logistical issues as contractors and additional staff showed up to help. The two system admins became major choke points in getting things done and the number of people needing their attention kept them from getting useful work done as well. Word of the attack was also spreading through the community and more offers of help were coming in. It was the "Mythical Man Month" at work.

-

Management started to assign roles to people and groups to provide food, create quiet spaces to work, track expenses, be gophers, develop a document for tracking work on systems, and more.

Week of 9/23: Payroll completed

It was Monday before the insurance company was notified because they didn't operate on weekends, but by that afternoon we were talking with the contractor they had hired for incident response. The incident response contractor had us install their preferred anti-malware software on all servers, run their forensic scripts on all infected servers, provide full access to our O365 email domain, install a network IDS system, and not delete any data or old server images. This work had to happen while we were still trying to get services restored. Even with all the extra work the incident response contractor caused, it was good because they had been through these events multiple times and assured us that we only needed to be concerned about Windows machines.

-

And most important of all: Payroll was completed on time.

Attack Aftermath

In a ransomware attack you first think in terms of hours, then in days, then in weeks, and finally (in a bad case like our's) in months as you get things running again. We had most services that end users notice up in a month and files restored in two months, but the long days continued into December, even with a contractor who had overseas staff that could continue building systems and running forensic scripts while we slept at night.

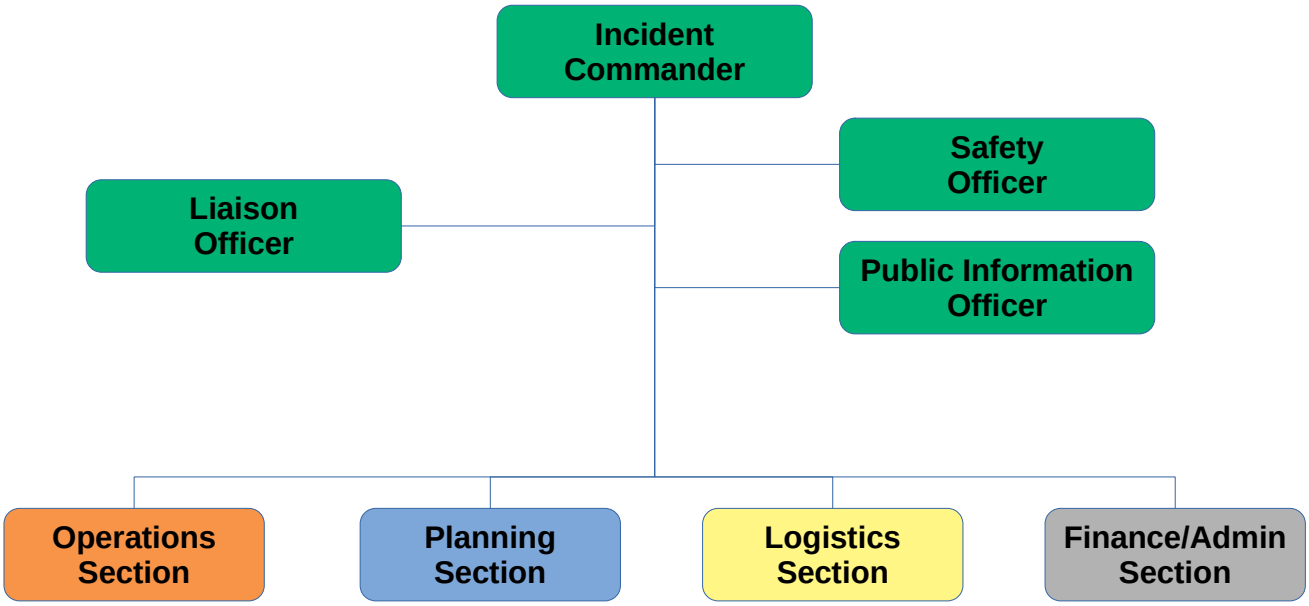
-

We have moved many more of our services to SaaS providers such as those for time keeping, library, and the food services POS. We have implemented a new backup solution with a technological 'airgap' and we are implementing a central logging and SIEM solution.

-

The ransomware attack also finally got us approval to fill two positions that had been funded previously, one for a Network Security Engineer. We have completed an external security review using the CIS-20 controls as a baseline and are in the process now of implementing their recommendations. This event has changed how we work in that security is now a district priority,

Lesson #1: Fill all these Roles



https://training.fema.gov/is/courseoverview.aspx?code=IS-100.c

During a ransomware attack you will need to fill all the roles defined in the Incident Command System which is used by governments and companies around the world. I recommend one liaison person for other departments and another for the contractors to assist in answering questions like when will services be up, who needs access to what, why, and when? The Public Information Officer will need to prepare communications for staff, students, parents, and the media. Yes, we had a TV truck at the Admin building several times. Logistics provides food, workspaces, and does the non-technical tasks. We found creating quiet rooms where the people could work uninterrupted was very helpful. The system admin who was rebuilding our Active Directory domain was locked in a room where only his supervisor could approve someone to disturb him until the rebuild was completed. Finance tracks all the costs for the insurance claim and figures out how to pay vendors until the accounting system can be restored.

Lesson #2: Relationships are Critical

I cannot stress this point enough. Without good relationships with contractors, vendors, and district staff, we would not have been able to recover our systems as quickly as we did. Our relationship with a local hosting firm provided 5 experienced system admins some of whom were overseas and a project manager. We used them for the forensic work, anti-malware installation, and many server rebuilds. A contract developer created a map between the SIDs and CNs that we recovered from the old Active Directory system which was critical in building the new one and restoring the file server.

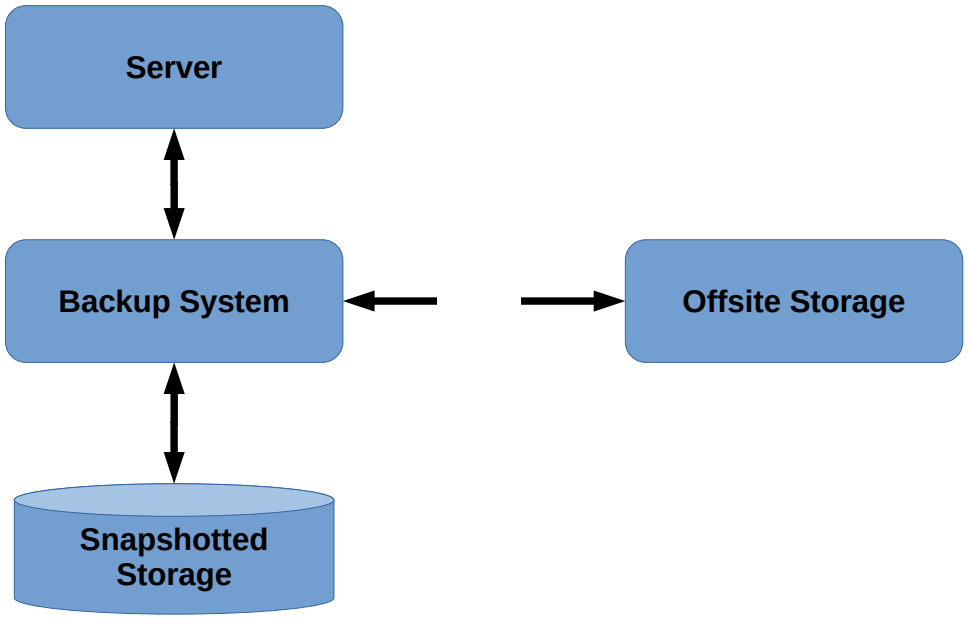
-

The student records vendor was willing to drop everything and complete a typically 6 month migration to their SaaS solution in 6 days. A parent who worked at Microsoft made sure we had access to the support we needed to figure out the Office365 syncing issues as going through normal channels was not successful.

-

Finally, our Management, Help Desk, and Instructional Technology teams were incredible at making sure the rest of Technology could focus on rebuilding our infrastructure. Anything we needed, they would make happen.

Lesson #3: Airgap your Backups



Make sure your backup system includes an airgap that is working 100% of the time. According to the incident response contractor, attackers have automated routines to find and corrupt backups of major vendors so you need an either a physical airgap such as removeable media or a technical one such our our NAS hardware snapshots. Because our backup system was not ‘airgapped’ 100% of the time all the attacker had to do was to render the file system it used inaccessible. Just a warning, apparently this is very easy to do with ReFS.

-

After you have been hit, you need to immediately create a new backup system in case you are hit a second time. According to the FBI, many ransomware targets were hit a second time a month or more later. We reinstalled our current backup software on a snapshotted file system which provided a technical airgap until we could replace it.

Lesson #4: Look for Informal Backups

If your backups are not accessible, you may have accidental backups in other locations. Look for vendors or contractors who did work for you previously and may have made a backup beforehand, or staff who support the systems and may have done the same. There is a good chance you will find some data somewhere.

We were lucky with the phone system as the support contractor had set up backups to a hosted service during our most recent update - we lost old voicemails but got everything else back.

Lesson #5: Insurance will Impact You

I was amazed at the impact our insurance group had on the recovery process. Once you involve insurance, you lose a lot of control.The insurance company's goals are not the same as your's. You want to get everything working again as quickly as possible. They want to make sure the attackers are off your network and aren't able to come back again, in order to minimize their payout. There is pressure to do what they say or they may not pay your claim. They dictated which incident response contractor we would work with for the recovery effort and also that we had to support that contractor in forensic efforts.

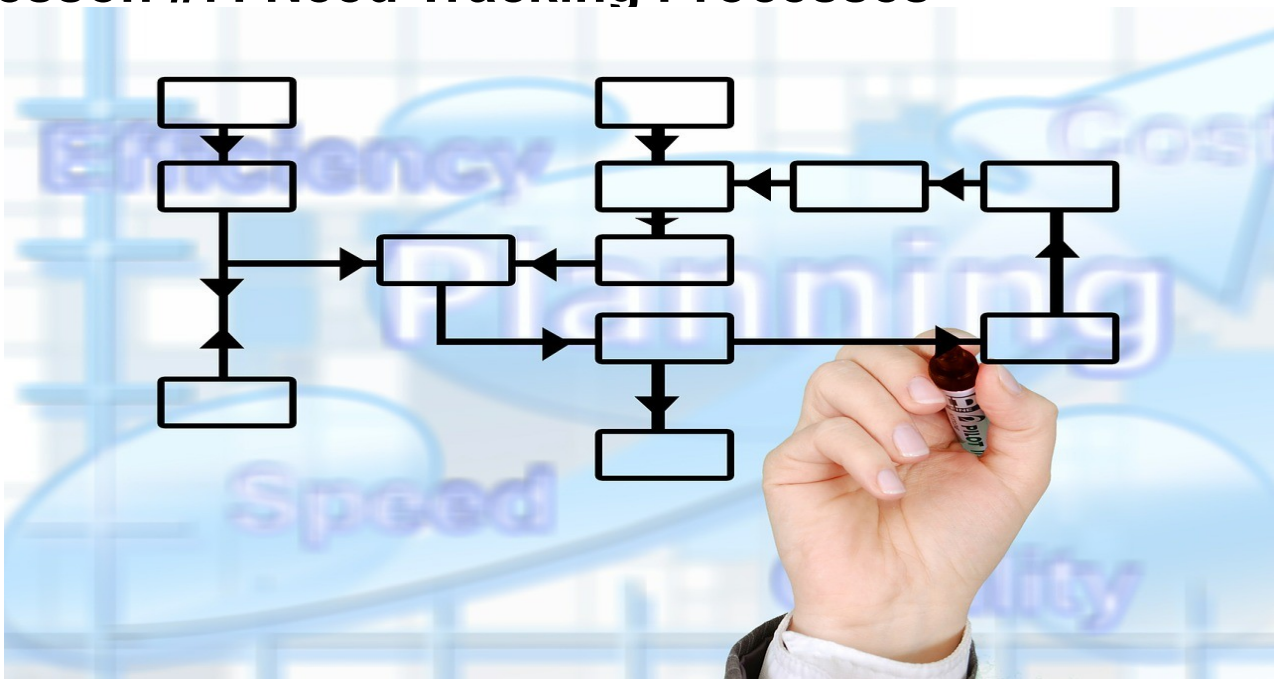
-

The insurance group also looks at the cost of rebuild vs cost of ransom. In our case if we were not able to get one or more of payroll, student information system, or phone services restored, we probably would have paid. Even so, if the ransom had been lower, we may still have paid because of the losses due to our food services POS. And yes, payouts are fairly common. The insurance company negotiated 4 ransomware payments for other customers during the first week after our attack.

Lesson #6: Forensics are Time Sinks

One thing the incident response contractor has you do it to run forensics on all infected machines to determine how the attack happened. Running forensics on 180 servers is very time consuming. You will need to create processes using isolated, private networks and virtual servers to run the forensics so you do not cause a reinfection. There was definitely tension between the incident response contractor wanting the forensic work done more quickly and us wanting to get systems restored. We could have never done this without the additional contractors and their overseas staff who could work during our off hours.

Lesson #7: Need Tracking Processes



You will need to create new processes on the fly for tracking your work such as the time spent for the insurance claim, what machines were built and need to be built next, what machines had forensics done, what services were still down, had been restored, and which were next to be restored. We ended up using Google spreadsheets for many of our tracking needs.

-

You also need to be able to show various interactions, such as services that depend on other services for authentication, or that depend on database servers for their data. This obviously defines the order in which you restore things, but also helps explain to administrative staff why some services are delayed in coming back up, why a server could be unaffected but the service is unusable (no login), or why suddenly a dozen services came back up at once.

Lesson #8: Get a Project Manager

You will need at least one experienced project manager to track what tasks are getting done and keep the focus on your most important tasks. This allows your technical staff to focus on recovery work. Any requests from outside to change the priority of tasks needs to go through the project manager so requestors are forced to take a serious look at their need versus all others.

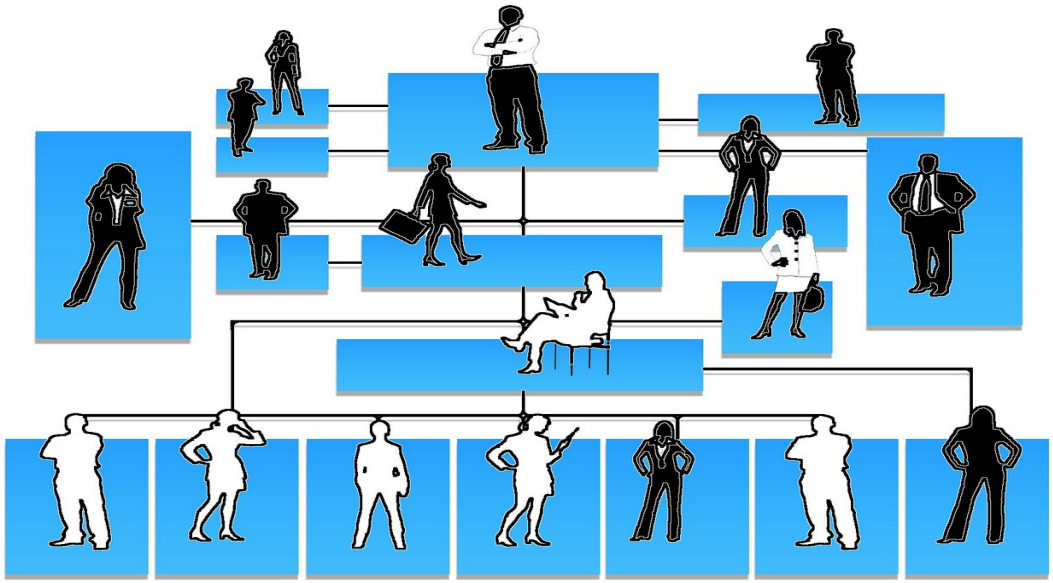
-

It is important to take a few minutes at the start and end of each day for a sitrep on what is going on, especially when there are multiple parallel teams working. Some staff may not be able to help with the most critical services, but there is lots work they can be doing such as assuring that workstations have the latest anti-malware software and are joined to the new domain.

-

Have a plan, stay calm and realize the plan will change - possibly frequently. The project manager the contractor provided was worth their weight in gold and I wish we could have had a few more.

Lesson #9: Under Staffing Hurts



Understaffing has several side effects - all of which are bad and really show up during a ransomware attack. A few of which are:

- Lack of cross training leads to many bottlenecks during recovery;
- Each staff person wears multiple hats so the one person supports VMWare, Storage, Backups, etc. What should they work on first?
- Projects tend to get only partly completed, such as our phone service upgrade which did not have backups configured yet;
- There is a tendency to build up "cruft" as things change - not completing documentation about changes or not deleting deprecated systems just in case you may need access to them;
- Systems get too far behind in patching and updates;
- Work is often pushed off to contractors and vendors so server staff aren't familiar with how the system was built or configured. We spent a lot of time tracking down the contractors that did previous installations to get information from them on rebuilding the service.
- With lack of documentation both of initial setup and of small changes made to systems, you are dependent on staff memory and oral tradition which is often fuzzy at best
- Staff may already be tired or stressed from the constant high workload, leaving less resilience for dealing with a major event;

Lesson #10: Need More Storage

When we were told that we could not delete the infected machines or encrypted data, we ran into a severe storage crunch. Can you create duplicates of all your servers and data on the storage you currently have?

-

On the file server we had a few major issues. First it was EOL so all we had was hardware support. We could not just revert to a snapshot as we were not allowed to delete corrupted data so we had to copy data from a snapshot (whoops even more storage needed). Actually a lot more storage needed because when we copied data we ran out of snapshot space in addition to normal storage space. We actually lost a bit of data before we figured out how to deal with this problem.

-

Also applying windows ACL's to the restored data is a non-starter as any change takes forever to walk the tree when you have 100,000+ files. New ACLs were required because we had an entirely new AD domain with different SIDs. We found the best solution was a script that recreated all the directories in the file system tree in a new location with the correct permissions and then copied the files into it. The only downside is all the files will now have the date that you copied them into it which will break some systems and confuse your staff.

Lesson #11: Lots of Trial and Error

It will take much longer than you expect as there is a lot of trial and error in rebuilding an infrastructure from scratch. You will run into many little unexpected things that increase the time needed ranging from ”is the attacker back on our network” to ”how do I rebuild this server", “how do I get a license for this system”, or “how do I restore the files with correct ACLs”.

-

There will be things you did only once or do infrequently that have to be re-learned every time, especially if you have staff turnover. There will be a desire to re-think some core design decisions. This is good, but takes you in a new direction that may require some research and testing.

-

There are also complex interactions between services that may not be fully documented or understood, or even processes running that nobody remembers. This can cause problems to appear later when everyone thought they knew exactly what needed to happen for the rebuild.

-

Finally, you will have to explain to other departments why things have changed from what they were told a day or even hours ago as you work through the trial and error process of figuring out how to recover your systems.

Lesson #12: Rebuilds Will Take Time

Spend time up front getting your virtual server templates correct - we did not because our windows admin was focused on the Active Directory rebuild leaving the new virtual server templates to much less experienced staff. Between this and the changes required by the incident response contractor, we ended up rebuilding some templates and servers multiple times.

-

You will need to track down media, licenses, and proof of purchase for the systems you are rebuilding. Some of our licenses took days to get from unresponsive vendors.

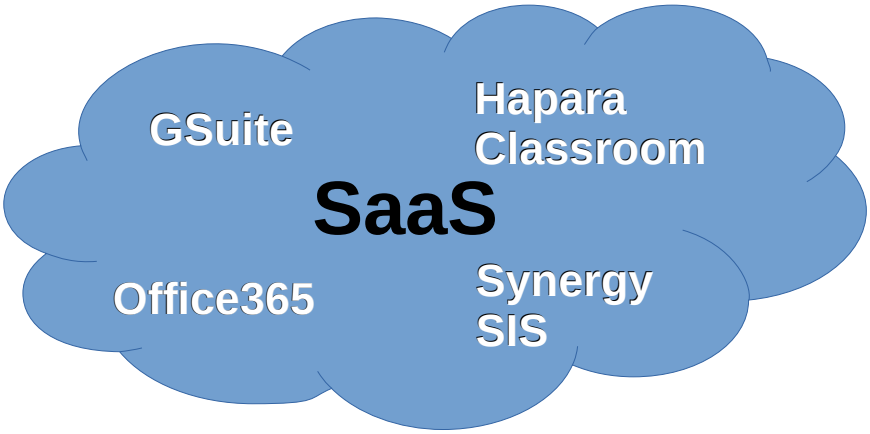
-

Take the time to build isolated networks either physically or in your virtual environment. We built an isolated network in vCenter where we could safely launch possibly infected servers to look at their disks.

Lesson #13: Clean up your Systems

We were able to use this event to clean up many of our systems. All windows and SQL servers were finally updated to newer supported releases and completely patched. Instead of restoring everything on file server, we only restored files people asked for. Some of our legacy systems were never restored as people found out they were not needed or the software was too old to work. This may make the recovery process longer, but it is worth it in the long run.

Lesson #14: Move Services to SAAS



If you can, move services to SaaS solutions, even if it is only temporarily to get through the recovery. This will reduce the number of servers your system admins have to rebuild and increase the number of people involved in the rebuild process thus speeding up the entire recovery. Our management decided to move the student information system from on-prem to a SaaS solution. This saved us from rebuilding 27 servers and, more importantly, meant the student information system could be restored and set up without going through the system admin chokepoint.

Lesson #15: Many Temporary Things

You will need to create temporary work areas on the file server so people can work while you are restoring the original file systems. We restored critical data to these work areas, then merged the data back into the original file system when it was restored. You will need to train people on how to access the temporary machines and file spaces.

-

You will need several temporary servers to run forensics, test anti-malware software,test database recovery, run limited versions of services, etc. until the final servers can be built and configured.

-

You will need temporary desk and office space for all the people who will be helping you. You may also need to take over space from existing staff to create quiet areas for those doing the most complex recovery work so they can focus or so they can work on speakerphone with tech support without interrupting others.

Lesson #16: Workstations

We had around 1500 windows workstation users that are primarily support staff (cooks, central office) and Career and Technical Ed teachers and students. We only had around 100 windows workstations infected which was great news, but we still had to install new anti-malware and check all windows workstations before they were allowed back on the network to assure no reinfections. Also because we built a new active directory domain, we had to rejoin all 1,500 workstations to the new domain and migrate their profiles over. This added up to thousands of hours of work.

Lesson #17: SCCM Restores

We spent several days attempting with Microsoft support to restore our SCCM server as we had a database backup, but because SCCM keeps an internal ACL list based on the SIDs from the old domain the database backup was not usable. and we had to rebuild it from scratch. This meant we also had to rebuild all the imaging and software packaging needed for the windows workstations.

Lesson #18: Surprise Applications

You will find critical systems that you had no idea they existed or were critical. A few that we ran into were:

- The food services POS system for our cafeterias stored data on local workstations that were not backed up so we had no idea how much money any student had in the system or if they owed us money. We also had no clue that Food Services sold over 10,000 meals a day, which amounted to $30K/day of business. In addition, this system is used to report meals provided for families that qualified for "Free and Reduced Lunch", which is used in reports to the federal government for funding back to the district. This turned into our 3rd most critical system due to the amount money involved.
- The Library system as keeps tracks of library fines and the transportation fuel depot system as it keeps tracks of fuel we sell to other local entities.
- Time-of-year surprises. We experienced a cold snap just after the attack. Instead of using the HVAC system to update all controllers at once, the HVAC team had to go to each site and plug into each controller by hand. Our intercom system, which also ran the school bells, was a similar surprise. At first we were told that it could wait because school bell schedules stay pretty much the same most of the year. However, a few days before the Daylight Savings Time change on November 3rd, it became critical as people realized that the time change would shift every bell by an hour. Same thing with the door lock systems.
- The reader board at the local football stadium. Not normally critical except that ESPN had decided to air one of our high school football games the Friday after the attack.

Lesson #19: Keep End Users Informed

Your end users will want to help as long as you are transparent with what is going on. They need to feel that their needs are being considered and that they are involved in the recovery. Let them know up front about file and service recovery timelines and be honest with them about your priorities in recovery. Ask them what is the minimum they need to keep their critical processes working so you can possibly provide them that more quickly. In the Food Services case, they changed to a offering only a few standardized lunches at a fixed price instead of allowing students to pick what they wanted to eat. This gave us a bit of a breather on rebuilding their system. They still had to record meal sales on paper, though, which resulted in a huge amount of data re-entry later on.

Lesson #20: AD Side Effects

We were fortunate because we were able to use opensource ldap tools to recover active directory SIDs and CNs when the normal active directory tools failed. However creating a new active directory domain meant a lot more work in restoring files and recovering the workstations.
-
In addition, our Office365 domain is provisioned and managed by syncing data from Active Directory through ADConnect, but now the SIDs did not match. It took 12 days of working with several people at Microsoft to figure out how reconcile the Office365 SIDs with the SIDs in our new Active Directory using the msds-consistency GUID. We were constantly running into throttling issues during trial runs and for the first complete sync. Services you have that sync from Active Directory may have the same issues.

We also had to rebuild all our GPOs from scratch.

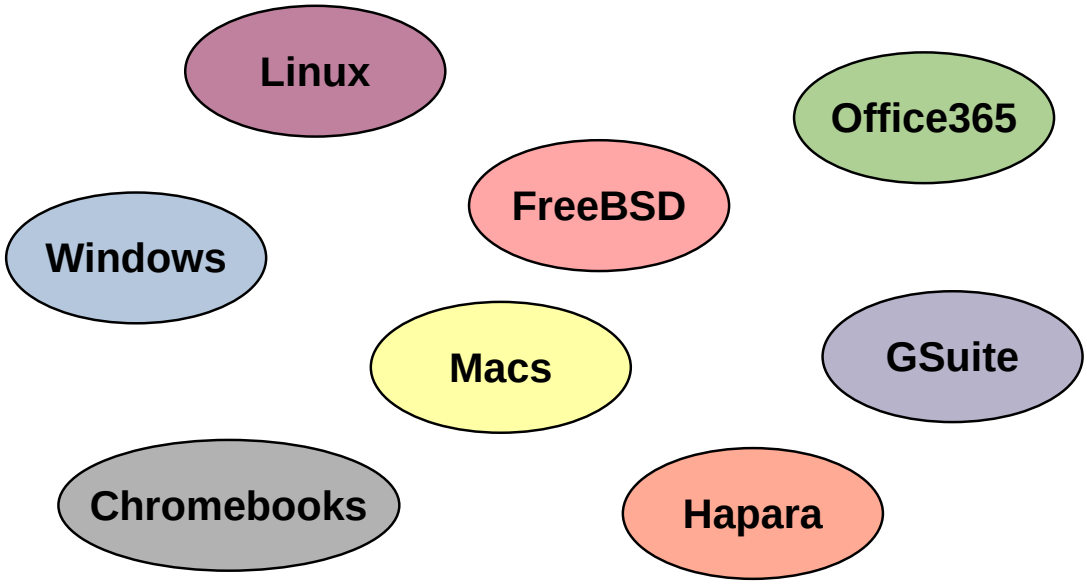
Lesson #21: Lock Down Admin Accts

One big factor that caused the attack on us to be so successful was that many staff accounts were also domain admin accounts. We were in the process of changing that, but not far enough.

-

We have now implemented the concept of superuser accounts (e.g ckacoroski-su) for all 'admin' work and use our regular staff accounts (e.g. ckacoroski) for for email and other ’user’ work. The -SU accounts cannot send email and any email they receive is forwarded to our staff account. As a quick fix for domain admins, we wrote a script that allows the senior system admins to add a -SU accounts to the domain admins group for a limited time such as an hour. We are in the process of replacing this script with a vendor supported tool.

Lesson #22: Heterogeneous is Good



Our district was primarily a Macintosh district 15 years ago. Because of that, many of our services run on non-Windows servers including DNS, DHCP, OpenLDAP which is our canonical directory. Most of our staff and students are on Mac, Chromebooks, and iPads. This was a primary factor in our ability to rebuild and not pay the ransom. While the loss of our Windows servers was a big hit, it did not take down a number of services that support instruction so school was able to continue. This was a both a blessing because most people were not affected and a curse as some of the senior management wondered what was the big fuss - email was working and most people are not affected - how bad can it be?

It was like a earthquake happened and 70% of our buildings (windows machines) were destroyed. The only thing that survived were some buildings (non-windows machines) and utilities (DNS, DHCP, NTP, etc.)

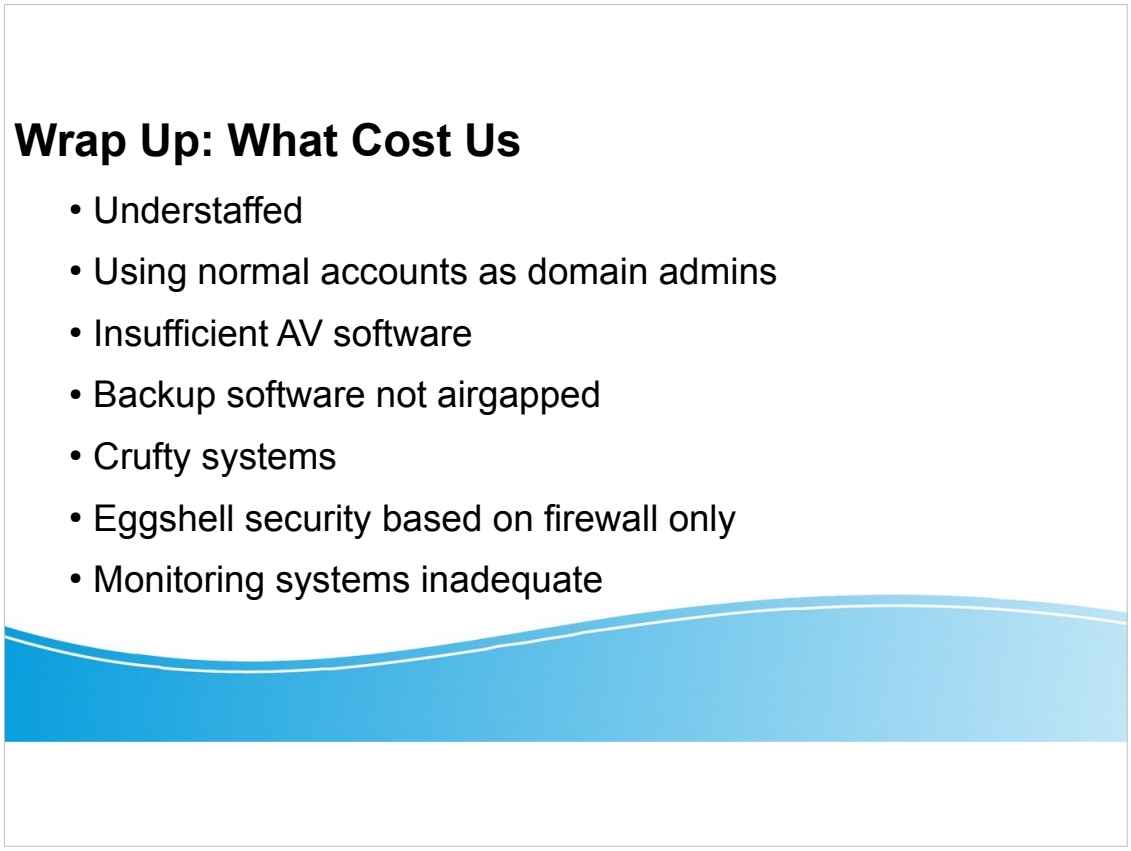
Lesson 23: Take Care of Your People

You need to make sure people take breaks and stay fed and rested. People will naturally want to work around the clock to get systems running, but recovery is a marathon, not a sprint, and tired people make mistakes. Thank them for their efforts - frequently - and celebrate the small successes. At times we were swamped with people who wanted to help - it is ok to tell them no. Our management did a great job in taking care of us during the recovery.

Cowbell whenever we recovered a system to celebrate the wins.

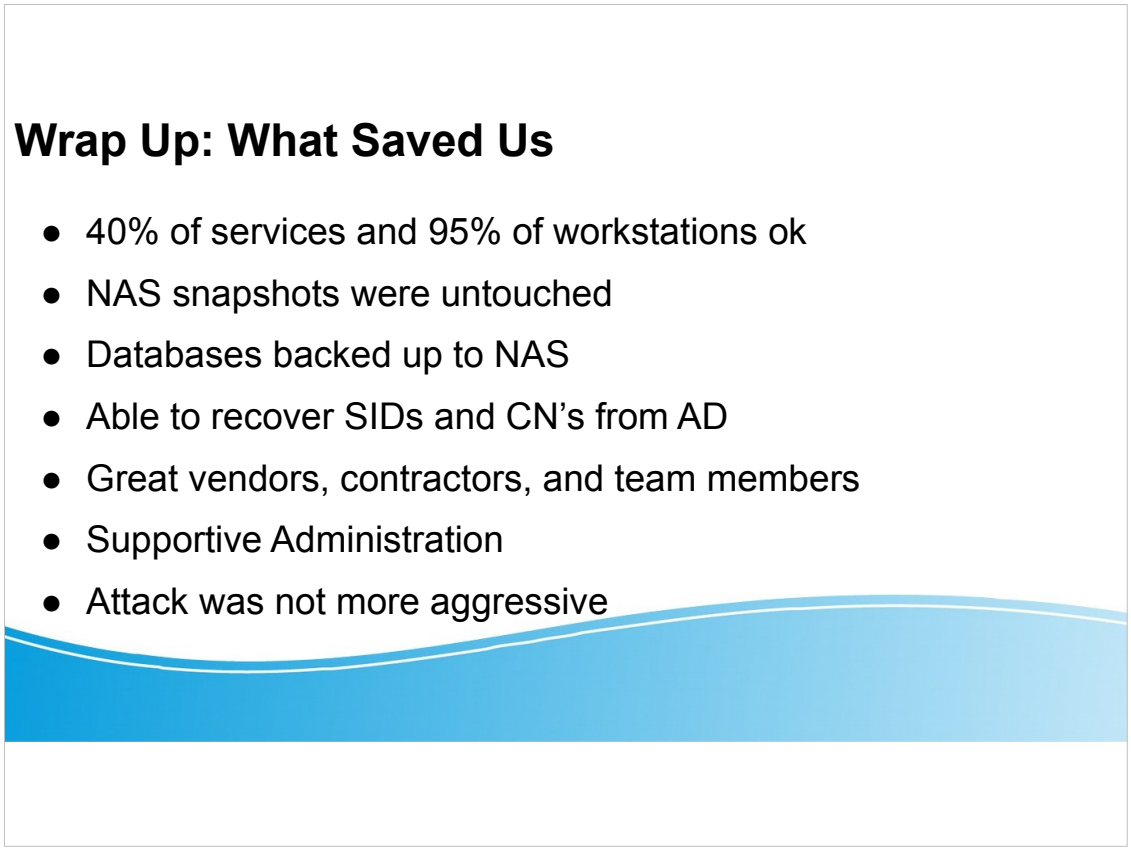
Lesson #24: Uncertainity impacts

One of the biggest issues you will face is that your infrastructure is no longer safe. Who knows what could be lurking on it or what backdoors had been left behind. Anything strange will make you jump as you wonder if the attacker is back on the network. You will spend a lot of time tracking down false positives - and it is worth the time. Several school districts were hit multiple times because they were not careful enough in rebuilding their systems and, as the FBI informed us, attackers will try again. It may be months or even years before you stop jumping every time something happens. Even 18 months later, we still feel a bit of panic whenever multiple servers start showing strange symptoms.

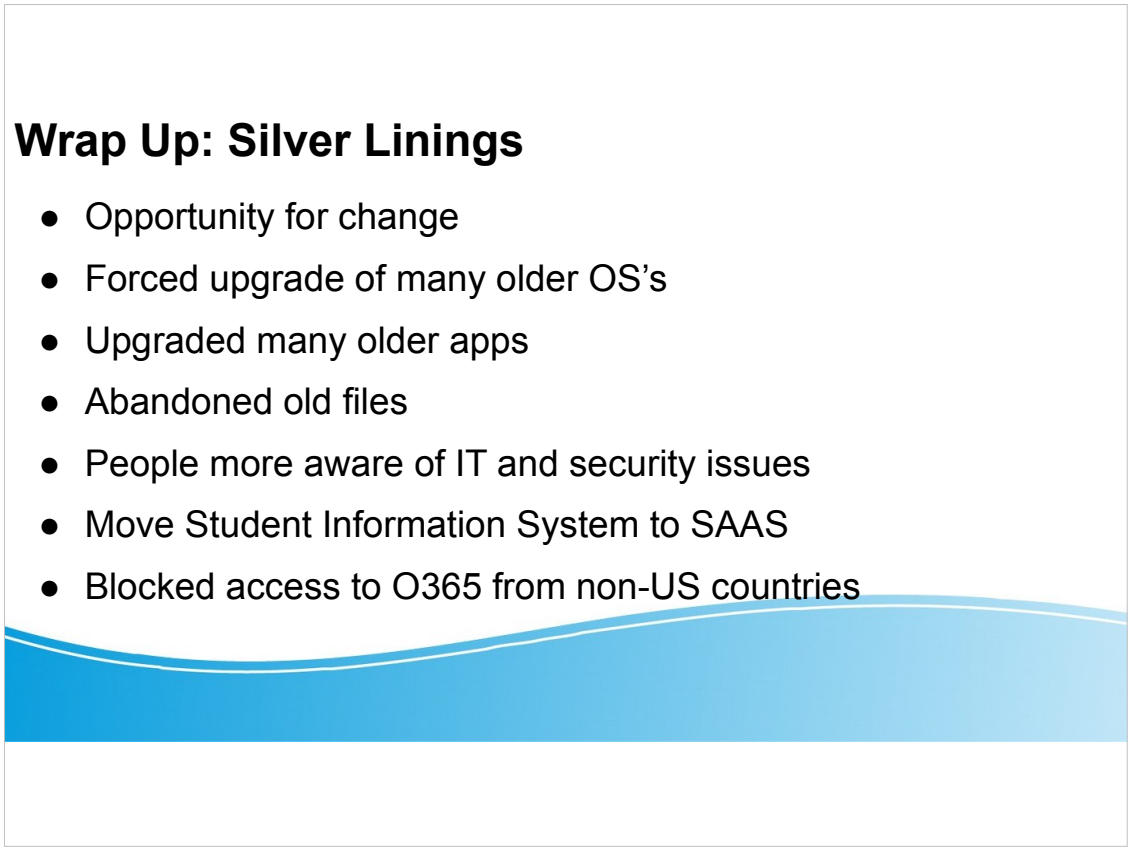


Being understaffed is the root cause of many of the factors that led to both our attack and its extent, leading to:

- security shortcuts, such as using normal accounts for domain admin access;
- no internal limitations between machines and dependent on the eggshell model with security based on a single set of firewalls;
- failure to properly configure our anti virus to provide adequate protection;
- system and log monitoring that was either not trusted or else limited by license costs.
- a lot of cruft in systems that slowed down our recovery;
- lack scenario game playing - what planned for an earthquake scenario, but not a ransomware attack.



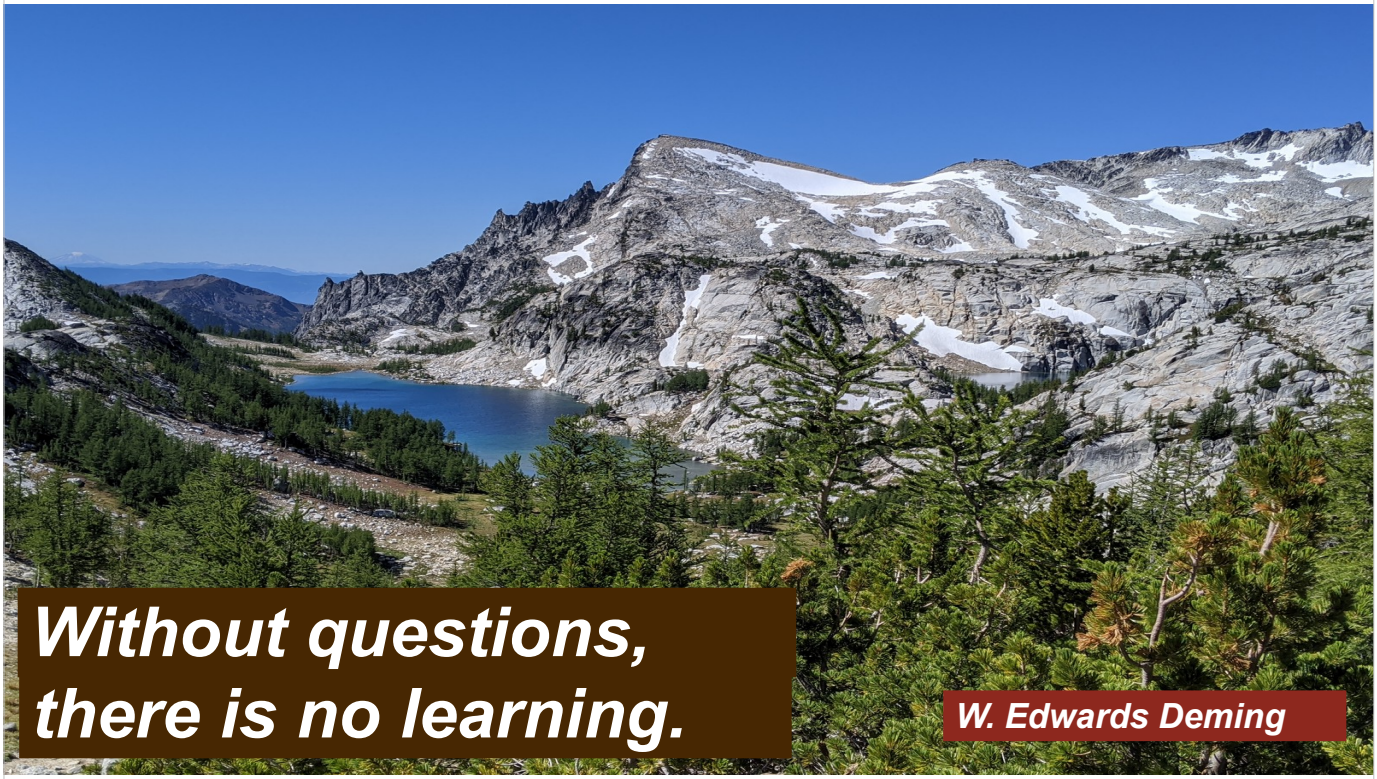
Most of our end users were minimally affected because we run a heterogenous infrastructure. Most of our data was recoverable either via snapshots on the NAS, from vendors, or from workstations that were not hit. We were able to recover the SIDs and CN's from active directory which enabled us to build a new one with correct users and permissions relatively quickly. The attackers were not more agressive in that they did not try to destroy snapshots, non-windows machines, or exfiltrate data. And, I cannot stress this enough, our relationships with our vendors, contractors, and team members are what enabled us to survive the attack.



The major silver lining from the attack is that everyone is much more aware of security and the dangers we face. This has enabled us to make make changes that would have been extremely difficult before it happened such as employee training on phishing attacks and a discussion of implementing multifactor authentication for employees.

-

We were able to retire all our windows 2003 and 2008 servers and upgrade many services to run the latest versions. All our servers were fully patched and we are working hard to keep them that way. We were able to clean up a lot of cruft by only restoring data that people asked for.



Questions?