



NO ONE IS SAFE FROM CYBERCRIMINALS

Precoat Metals shares their cyberattack experience and steps for recovery

On May 12, 2021, the president signed an “Executive Order on Improving the Nation’s Cybersecurity,” but ultimately, it’s up to you to protect you or your company from being the next target.

In this candid and compelling interview, Vice President of Business Information Systems Rick Miller offers an insider’s view of the cyberattack Precoat Metals experienced from a before, during, and after perspective. It may just keep you and your business from a similar fate.

When did the attack occur and how did you first know?

I’ll never forget the date. It was Tuesday, April 28, 2020. The director of IT called me at 5:30 in the morning and said that we had been hacked and we couldn’t connect to anything on our network.

The attack was first discovered when a coating line operator saw a mass closing of applications and his PC unexpectedly shut down. Seconds later, his computer began to reboot, and then, he was staring at a bright blue screen with the looming message, “Your network was hacked . . . If you decide not to cooperate, your sensitive data will be shared with the public.”

Within minutes, we realized the same thing was being reported at multiple locations across the plant. As the hours passed, we learned how severe the attack was.

What type of attack was it?

It was a ransomware attack, where a perpetrator seeks to encrypt your data and encrypt your backups. The only way to unlock or recover the data is to pay them money to get your files back.

What ransomware were you hit with?

It was called DoppelPaymer, and it was successful in encrypting a small portion of our files making them unrecoverable. We experienced no data exfiltration, and all the targeted systems were Microsoft-related systems and software.

A related piece of software they used is called Dridex. It gets deployed onto the network to scan for vulnerabilities and is usually delivered via email.

Millions of malicious emails get sent every day by online criminals hoping someone opens them. It only takes one person to trigger the malware. Later, it activates the ransomware which paralyzes your systems and files.

They offer to give you the encryption codes (to unlock your files) if you pay a lump sum. You are typically instructed to pay in Bitcoin.

What type of infrastructure did you have in place prior to the attack?

I’d describe Precoat’s pre-attack infrastructure as normal, well-structured, and efficient. We had 15 locations connected by one network, a centralized data system, and common applications used by all.

We also shared a centralized Cisco VoIP phone system. Email, file, and print servers were set up at each location. Backups were maintained locally.

We had a relatively new (six-month-old) IBMi primary server, and both Windows 7 and Windows 10 systems were in use throughout the company.

What steps did you take when you first discovered the threat?

The first few hours of the attack could be described as chaotic and maybe even frantic. We couldn’t tell what was broken, let alone how to identify the problem or how to implement a solution.

As time passed, we learned more about the scale of the attack, and we made some

Precoat Metals is a provider of coil coating services with 60 years in the industry, a DASMA Member, and as of April 2020, a victim of a vicious ransomware attack.

The cyberattack epidemic has hit both our industry and the mainstream with the recent attack on petroleum distributor Colonial Pipeline. These attacks prove that no company is safe, and if targeted, there could be far-reaching consequences.



Rick Miller

We knew the impact to our business was significant and we didn't have a solution. Plus, we were staring at the possibility of information gaps for an undetermined amount of time.

By 11:00 a.m. ET (after six hours of extensive evaluation and attempts of recovery), it was clear that mitigation of the attack was outside the skillset and the available tools of our IT team. Clearly, we needed help.

Who did you enlist to help?

We hired a third-party company that specializes in cybersecurity and protecting companies from this type of breach. The company we used, Cybersafe Solutions, is located in Washington, D.C., and was recommended to us by our sister company Chromalloy.

By 12:30 p.m. ET the day of the attack, we had contracted with Cybersafe for help. *See Cybersafe Solutions side bar.*

What did Cybersafe do?

They have seven years of experience with these type of ransomware attacks. Their immediate goal was to protect what wasn't already affected and try to recover and remediate.

At the time of the attack, Precoat had 14 manufacturing locations plus a headquarters facility that were all sharing the same collection of data, so this was a huge undertaking.



Precoat Metals

What systems got "hacked"?

We determined that all of our Microsoft Windows servers were hacked. The primary IBMi mainframe server and Linux servers were not impacted by the attack. This allowed us to keep operating.

We also discovered that our customer portal, Coil Zone, that we rely heavily on internally and externally, appeared to be working normally. Unfortunately, reporting capability, which typically handles the distribution of several thousand reports each week, was inoperable. It took us eight days to re-establish this functionality.

As mentioned, we had turned off the VPN connection at the onset of the attack. This was good because it could have potentially provided a path for our hackers to reach more devices. This decision may have limited the overall effect of the attack.

What did the recovery process look like?

The path to recovery was exhausting. The Precoat and Cybersafe teams worked 16 to 18-hour days during the first two months after the attack, and we scrambled to return to normal for our customers.

Many company PCs were encrypted, so over the next three to four weeks, we replaced the hard drives and then rerouted the updated devices to various plants. We worked to contain the attack, recover our servers, and establish a more robust security protocol moving forward to avoid further contamination.

We were able to recover the vast majority of our files by recovering them from backups. According to the Cybersafe folks, "We were extremely fortunate that our backup servers were not affected."

What additional security did you implement?

Cybersafe implemented their Threat 360 platform, which included a SIEM, Intrusion

continued on page 40

key decisions early on. Due to COVID-19, we were fortunate to have roughly 115 employees working from home. With user authentication unavailable and preventing a log-in, we turned off VPN access as a precautionary measure.

Which systems were affected?

We learned that our email was down, phone use had been compromised, internal and external reporting was completely broken, and that we had no access to any of the shared files on servers. Communication was a challenge, to say the least.

We eventually discovered that our IBMi and Linux servers were fully functional and were not impacted in any manner. This was great news because throughout this crisis, this enabled us to continue with normal operations at our plants.

How did your IT team deal with the issues?

Everybody wanted answers and we simply didn't have them. To establish communication, we devised a workaround by asking employees to set up Gmail accounts. Aside from that, the in-house actions we took proved ineffective.

Detection, and a more sophisticated endpoint security software called Sentinel One which was deployed to all devices (PCs, laptops, and servers).

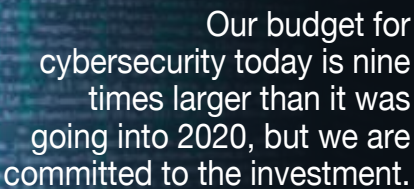
They were also able to provide a Sentinel One version for use on our Linux server. This heightened our overall level of security and helped keep additional hacks from being effective.

In addition to expiring all passwords, we completely overhauled our pre-attack structure and centralized both user authentication and Email. The approach to implement new systems sped up our recovery and improved security. Five days after the attack, the email and EDI function were back to normal operations.

We also implemented a more sophisticated and more expensive version of Barracuda for spam and web filtering. We continue to evolve our backup strategy.

How much does your company spend on cybersecurity?

Our budget for cybersecurity today is nine times larger than it was going into 2020, but we are committed to the investment. We also recognize that these steps minimize the risk. Eliminating the risk is not in the cards for anyone.



Our budget for cybersecurity today is nine times larger than it was going into 2020, but we are committed to the investment.

How long were you down?

All plant operations continued as normal during the attack. We were extremely lucky. Some companies without the support system we had would be out of business.

We were able to establish normal functionality with all applications and systems for our customers eight days after the attack. Behind the scenes, the work remained extensive for several months, and the team continues to do clean-up work periodically.

Our cyber partner has identified several new hack attempts using our improved network monitoring systems. It is clear we are still being targeted, but our newly added protection systems are working.

The wounds of the attack have healed, but the scars remain.

What do you know about the online perpetrators?

We know that they are of Russian origin, well-known in the cybercriminal world, quite sophisticated, and well-funded. This group has direct ties to the Russian government and even have a help desk to assist with the ransom payment. This is an actual business, criminal in intent, but it is still a business.

If you pay a ransom, could your files be encrypted again?

No one would ever pay them anything if they had a reputation of continuing to encrypt the same targets and files.

When you first see the offer to pay the lump sum, you think, "How do I remedy this?" You have to decide whether to pay them a bunch of money and hope they play nicely, or rebuild your system from scratch.

Do you think larger companies are more at risk of being targeted?

Absolutely not. Online criminals are not just targeting big businesses for payouts, they are targeting everybody. Smaller companies are more vulnerable and at risk of losing everything because they may not have the resources to recover.

Some low-level online criminals are even sharing the ransomware code to other bad guys, which in turn increases every company's risk of getting hit.

What would you recommend that companies do right now to protect themselves?

I encourage business owners to investigate their company infrastructures to make sure you are doing everything you can to prevent this type of threat. Determine your level of vulnerability.

Keep your hardware up to date with system updates and security patches, both servers and user devices.

Also, we think the Cloud is a great solution. About two months ago, we migrated to Office 365 in the Cloud (versus on-premise Microsoft Exchange). The Cloud-based systems help keep the software current and features email risk mitigation tools.

How can companies better prepare their employees?

Education and phishing training are a good start. Even with the best training, you should assume that someone is going to

click on something they shouldn't. I tell employees if you don't know the sender or if it looks unusual in any way, you don't need to open it.

We continue to test our employees. Sometimes we bait them with fake emails to see if they will click on an unverified link or file. Surprisingly, after extensive employee training on how to identify suspicious emails, we still have employees click on our test emails.

Also enlist experts to help counter the threats. Static defenses don't hold up well to dynamic offenses and online criminals are becoming more sophisticated every day.

What did you learn?

We are all targets, and we are constantly in the crosshairs of threats. Even if you are keeping your programs current and updating them regularly, the reality is that the bad guys are already working on something new to infect your files.

Microsoft creates patches to combat the threats online criminals are using to disrupt your systems, but the patches are always chasing the threat. It might be too late.

Why did you want to share this story?

We wanted to share our experience to help educate other companies about what we learned throughout this process. We also wanted to provide details about the security we implemented.

We hope that by sharing this information it may keep other businesses from a similar fate. We also wanted to increase the general awareness about this very real threat.

Do you have any final thoughts?

Don't assume it won't happen to you. We mistakenly thought our company is not one a bad actor would want to harm. We're not a retail or banking company; we just paint and process steel and aluminum coils.

Bottom line: If you exist, your company could be targeted. You must have a plan if this type of threat occurs and continue to update and test your plan. Also, backups, backups, and more backups, and it's best to have some of them offline.

Great resources for threats and mitigation: FBI and CyberSecurity and Infrastructure Security Agency (CISA).

Have you or your company experienced any type of cyber fraud or a cyberattack? Please email vicki@vjonesmedia.com to share your story.

“Cybersecurity is not an IT issue. It’s a business risk that can impact your bottom line.”
— cybersafesolutions.com



Keith Strassberg,
Cybersafe Solutions, COO

CYBERSECURITY IS NOT OPTIONAL

Cybersafe experts explain why

Working with a specialized company like Cybersafe Solutions was the key to Precoat Metals’ path to recovery. Cybersafe experts are trained to identify security incidents, risk exposures, vulnerabilities, and indicators of compromise (IOCs). We spoke with Keith Strassberg, Cybersafe’s chief operating officer, about the value of partnering with cybersecurity experts.

How did Precoat Metals’ decision to partner with Cybersafe within the first six hours of the attack help mitigate the damage?

Bringing in a partner with expertise in recovering from Ransomware attacks helped Precoat organize their response, identify and prioritize tasks, and immediately improve their security posture, which ultimately led to a quicker resumption of normal business operations.

What services does Cybersafe continue to provide Precoat?

Cybersafe now provides Managed Detection and Response services for Precoat. We monitor their laptops, desktops, servers, networks, email, and cloud infrastructure to detect and contain anomalous activity and threats before they can disrupt or damage Precoat’s business.

Which type of businesses do cybercriminals typically target?

In simplest terms, threat actors target businesses of all shape, size, and industry. Their goal is to profit from their activities, and any company — big or small — presents an opportunity for them to make illicit profit.

Why is it important for companies to implement cybersecurity before an attack?

It is far costlier to recover from data breaches than prevent them. Ransomware attacks disrupt businesses for weeks, even causing some companies to close, and problems can linger for years. Plus, there is no guarantee of a full recovery or that some data isn’t lost.

Implementing the tools and resources to prevent and mitigate cyberattacks at the earliest possible indication greatly reduces business risk. I often tell people that a small fire will quickly become a big fire if no one is paying attention; the same applies for a cyberattack.

Most businesses severely underestimate the cost of downtime and overestimate their ability to recover from ransomware. We find that most Disaster Recovery plans are not typically designed with ransomware in mind. Therefore, it also becomes damaged when ransomware strikes, which can inhibit a timely recovery.

How prevalent are ransomware attacks today compared to two years ago?

Ransomware attacks have grown in both their scale, speed, and sophistication. The frequency and costs associated with such attacks are orders of magnitude above where they were even just two years ago.

Threat actors employ new tactics to extort businesses, including public shaming, data exfiltration, and disclosures of company secrets. Even if a company has good backups and can restore systems, they will still have to spend significant time and money dealing with legal issues surrounding their data being exfiltrated.

Do you ever recommend paying the lump sum when hit with ransomware?

There is an ongoing debate about ransomware payments. There are active government efforts to make it illegal for an organization to pay a ransom, and insurers are removing ransomware payments from their coverages. The logic is that without the payments, these organizations will not have the funds to continue their attacks.

Ultimately, the decision to pay a ransom is a personal decision for the specific business impacted. If payment for hopeful decryption is the only option for a business to recover, then it’s an obvious decision.

Does common virus protection software offer enough protection?

Absolutely not. Virus protection is only one piece of a cohesive cybersecurity program. Even the very best virus protection program is not 100% effective.

Are there affordable cybersecurity plans for companies of all sizes?

Yes. Cybersafe’s monitoring services are designed, customized, and scaled to match any business’ cyber risks at reasonable prices. There is a return on investment that may not easily be seen as a line item, yet when compared to the potential costs of suffering an incident without protection, that ROI does stand out.

How can people and business owners learn more?

There is a wealth of cybersecurity information out there. Most organizations starting out would benefit from learning about one of the leading cybersecurity frameworks such as NIST or the Center for Internet Security Controls Framework. That will give them an idea of how the experts approach the cybersecurity problem. ■