OUT IN FRONT PLAYBOOK

AUGUST 2021

EMBER™

EMBERIT.COM

THE FOLLOWING CONTENT MAY BE CONCERNING

THAT'S WHY WE'RE HERE

Part of being a security company - and a trusted partner for our clients - is keeping our own eyes on cyber security trends and developing plans to stay out in front of emerging threats.

The **bad actors** within cyber security are constantly evolving, devising new threats, and targeting new companies and industries. Recently, we've seen an increase in threats that we would qualify as cyberterrorism - the use of the internet and technology to conduct acts that result in significant harm and are built around political or ideological goals.

n. Any entity that is partially or wholly responsible for an incident that impacts a company's security.

It is easy to write cyberterrorism off as "not a threat for my business" but we've actually seen the repercussions impact everyone from Fortune 500 companies to small businesses to individuals. While that is an unnerving thought to come to terms with, take comfort in the fact that we are here with the sole focus of keeping you informed, prepared, and out in front of threats as they evolve.

Matt Toto,
Founding Partner & Chief Information Officer
mtoto@emberit.com

THREAT SPOTLIGHT

GLOBAL CYBER THREATS

The world has changed drastically in the face of a global pandemic - with everything from purchasing behaviors to security being impacted by the long term effects of our response to an external threat. In the realm of cyber security, we've seen a drastic increase in the number of **ransomware** incidents as well as expansion in who is vulnerable to attacks. Everyone from large infrastructure organizations to small businesses have been targeted in the past year, making cyber security processes and practices more important for businesses of all sizes as we look ahead.

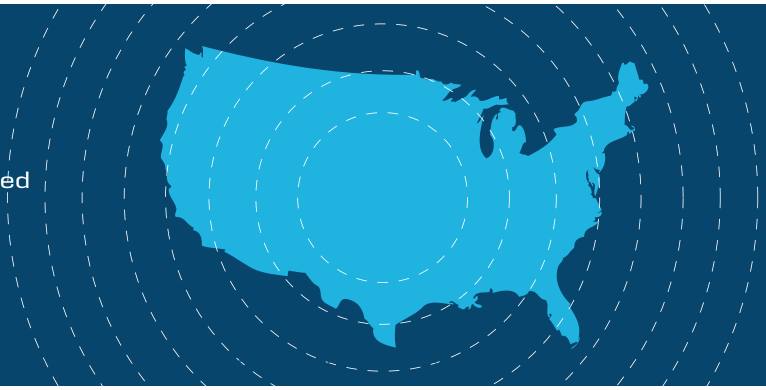
One real-world example of the potential impact of cyber attacks is visible in the now infamous, Colonial Pipeline attack. In May 2021, the Colonial Pipeline, one of America's largest pipelines and supplier of 45% of the oil for the east coast was hit by a coordinated ransomware attack and forced to temporarily cease operations, leaving many across the eastern seaboard without access to gasoline.

This attack was perpetrated by foreign actors looking specifically for financial gains but it underscores the vulnerability of our daily activities to the threat of outside attacks. In addition to the shut off of access to valuable oil reserves, the attack resulted in wide market speculation and declaration of a State of Emergency.

It may seem difficult to see what the Colonial Pipeline attack means for individual businesses, but in reality, this

n. A type of malicious software (or malware) designed to block access to systems or data until a ransom is paid.

69% of breaches + cyber attacks on the USA in 2019 were perpetrated from outside the country



Source: DataProt.net

IN 2020, RANSOMWARE ATTACKS SURGED BY 150%

WITH THE AVERAGE PAYMENT SIZE INCREASING BY MORE THAN 170&

Source: ThreatPost.com

attack helps us to see both how impactful a ransomware attack can be as well as the ripple effects of any attack that is made. A security breach in your company may not shut down a major oil pipeline, but it will have far reaching consequences within your organization that will likely impact your business.

In addition, cyber security issues are often more detrimental to small businesses that aren't as prepared to handle the fall out or don't have processes in place to deal with attacks. Many small businesses are caught off guard by cyber security issues and some are even forced to shut down their business because of the lasting impacts.

> "This [attack] underscores the threat that ransomware poses to organizations regardless of size or sector. We encourage every organization to take action to strengthen their cyber security posture to reduce their exposure to these types of threats."
>
> The Cybersecurity and Infrastructure Security Agency

As the world becomes increasingly connected and we see technology playing a larger and larger role in the operations of many companies, it will be crucial that we all prepare for cyber attacks and utilize best practices within our own organizations to help prevent widespread impacts and shutdowns. While there is no one foolproof strategy to avoid cyber attacks, there are steps that organizations can take to mitigate risk, prevent attacks, and increase the resilience of their team.

[1] 2019 *Data Breach Investigations Report*, Verizon Business Ready

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Eastown Pistons is a manufacturing company that creates pistons for 70% of leading automotive manufacturers, supporting and supplying the parts that companies need to build new vehicles. They've grown quickly in the last few years, adding offices throughout the country as well as operations outside of the US. They have good internal policies when it comes to security but updates to their protocols have taken a back seat to hiring and growth.

When the Eastown Pistons leadership decided to open a new processing location and transition their internal operations software within the same time period, they unwittingly opened their systems and processes up to bad actors. Foreign hackers slipped in through a patch in the software, collected valuable customer and payment information from Eastown's customer database, and demanded a ransom for its safe return.

The attack caused operations to shut down for multiple weeks and rippled through the economy, increasing demand but diminishing supply of new vehicles.

EXTRA CURRICULAR READING

Click the titles below for further information from resources we trust.

Protecting OT systems with IT collaboration
techradar.com // 06.26.20

Gartner: Surge in company cybersecurity committees predicted
businesschief.com // 01.31.21

Cybersecurity Risks
https://www.nist.gov/ // last revised 02.28.19

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THREAT SPOTLIGHT: GLOBAL CYBER THREATS

PLAYBOOK

6 TIPS TO KEEP YOU OUT IN FRONT

CLOSELY MONITOR AND MANAGE PROGRAMS AND PROCESSES TO AVOID GAPS IN PROTECTION

Most software programs go through periodic updates to keep them up to date and to keep you protected against external threats. Make sure your team is keeping your software patched, up to date, and relevant.

PROVIDE SECURITY TRAINING TO FOCUS ON EXTERNAL THREATS

Regular and consistent security awareness training is critical. Monitoring awareness and understanding of cyber threat risks can be the best prevention of attacks. Periodic ransomware and phishing simulations can provide clues about compliance.

MONITOR POTENTIALS ATTACKS

Even the best protected organizations will deal with attempted hacks and breaches. Deputize a member of your team to identify incoming threats and report on trends.

USE INDUSTRY SPECIFIC PROTECTION

While every company is susceptible to cyber attacks, not every industry deals with the same threats. Keep an eye on the types of attacks that are most likely in your industry and build safeguards to protect against them.

CREATE AN IN CASE OF EMERGENCY PLAN

Proactive cyber security hygiene will help to protect your company but no prevention techniques will prevent 100% of attacks. Create an internal process for how your team should handle attacks as well as a plan for communicating with internal and external stakeholders.

CONSIDER A SECURITY PARTNER

Keeping your company safe is more than just a one-person job. Bringing in a third-party resource can help you to uncover threats specific to your company, industry, and location and help to prepare both yourself and your team for these attacks.

FEATURED PARTNER SOLUTION

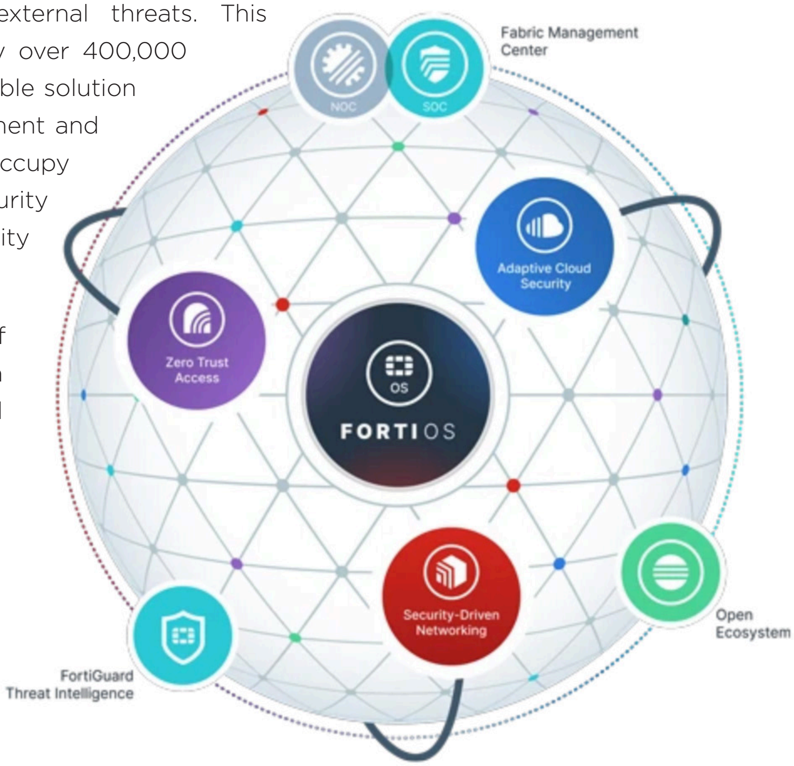
FORTINET®

EMBER employs Fortinet to help companies get ahead of their security concerns by offering comprehensive network security and endpoint security products unlike any other. Their always-on Security Fabric provides a reassuring guardrail for organizations with continuous analysis of network risks and by providing automated adjustments in the face of those risks.

Fortinet's FortiGuard Labs uses AI technology and machine learning systems to process and analyse more than 100 billion events each day and to give their customers actionable insights that can make a difference in day to day protection.

In addition, Fortinet has created a firewall platform to help enterprise clients protect their organizations from external threats. This firewall, FortiGate, has been used by over 400,000 organizations because it offers a flexible solution that can be made to fit any environment and industry needs. It also happens to occupy the #1 market share position for Security Appliances and to be used in the majority of Fortune 500 organizations.

Fortinet offers customers a piece of mind, updated security, and a plan to address cyber attacks with digital protection.



FORTINET SECURITY FABRIC

THE INDUSTRY'S HIGHEST-PERFORMING NETWORK SECURITY OPTION

OUT IN FRONT OF

Network Security

WHAT FORTINET DOES

The Fortinet Security Fabric is the industry's highest-performing cyber security platform, powered by FortiOS, with a rich open ecosystem. It spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications.

INDUSTRIES SERVED

- ▣ Education
- ▣ Healthcare
- ▣ Financial Services
- ▣ Manufacturing
- ▣ Entertainment
- ▣ Media & Communications
- ▣ Pharmaceutical
- ▣ Government
- ▣ Hospitality
- ▣ Retail
- ▣ Utilities
- ▣ Technology

KEY FEATURES

SECURITY-DRIVEN NETWORKING
ZERO TRUST ACCESS
ADAPTIVE CLOUD

BEST FOR

COMPANIES OF ALL SIZES LOOKING FOR ALWAYS-ON PROTECTION, BUT ESPECIALLY LARGE AND DIVERSIFIED ENTERPRISES

THE HUMAN FACTOR

OUT OF OFFICE (BUT NOT)

KEEPING YOUR BUSINESS AND YOUR DATA SECURE AS EMPLOYEES RESUME TRAVEL

The working world is constantly evolving. In the past, you may have been able to keep your employees - and their devices - confined to a single location where you could control firewalls, networks, and security processes. These days, not only are employees much more likely to be remote but they're also taking their work with them on the road. Building a Bring Your Own Device (BYOD) policy can help secure your data and give your organization the opportunity to take advantage of improvements and efficiencies that come along with BYOD.

Not convinced that personal devices should be part of your cyber security plan? Here are a few stats that may change your mind:

- **In 2020, there were 10 billion personal devices in use**
- **67% of employees use their own devices at work (even if they're told not to)**
    - **Only 39% of companies have a BYOD policy**

These numbers almost guarantee that your employees are using their personal devices to access company data. Even when your employees have your best interests at heart, they may be inadvertently putting you at risk by using their devices on insecure networks or not practicing the best security behavior on their own devices. Having a policy and guidelines in place not only protects you but helps them understand best practices.

Looking at the risk associated with personal device usage, it might seem better to simply avoid the whole matter and require employees to only use business devices, but let's take a look at the upside of BYOD:

- **95% of organizations allow personal device usage in some way**
- **Employees who BYOD work, on average, two additional hours per day and send an additional 20 emails per day**

And, let's be honest, some of your employees will use their personal devices even when you don't want them to, so it's better to be prepared.

The good news is that there are a number of ways that you - as an employer - can help both your employees and your organization to stay secure and take advantage of the benefits of BYOD. Use the work sheet on the next page to get started!

YOU'RE GOING TO WANT TO KEEP THIS PAGE

BYOD WORKSHEET

Use this guide to kickoff your own BYOD protocol and reach out to EMBER to build a comprehensive solution.

□ **Make sure your policy covers ALL of the devices used by your employees.**
To ensure you're not missing a single phone, laptop, or tablet, create an anonymous poll for your employees to log the devices they use and for what purposes. Polling them regularly will help you keep your BYOD technologically current.

Device	Brand / Model

□ **Designate ONE person or department to own the BYOD policy.**
A chief BYOD deputy will be responsible for creating and keeping your policy up-to-date. Equally important – they will also be the go-to resource for any questions your employees might have. Create a clear and easy way for employees to inquire if they have questions or concerns about the ppolicy and how to stay compliant. Two-way communication is key to keeping threats at bay!

BYOD Deputy: ______________________________

□ **Train your entire team on cyber security trends and your internal policies.**
Every employee is responsible for keeping your business safe. If your last training covered flip phones and desktop computers, it's time for a refresher. Schedule these trainings regularly and use each one as an opportunity to review and update policies.

Next training: _______ /_______ /_______ **Topic:** ______________________________

□ **Have a mitigation and action plan in place in the event that any of your employee devices trigger a breach.**
Protection alone won't solve all your problems! Include an outline of how to escalate issues and what to do in case of breach.

ONE LAST NOTE: When your BYOD plan is done, it's not done! Technology and threats never stop evolving, so your plan is only as good as how up-to-date it is.

Plan last updated: _______ / _______ / _______

IN REAL LIFE

A fabricated-but-plausible cautionary tale

This scenario is a work of fiction. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

John Carter is an operations manager at a Boston-based software development company, specializing in healthcare applications. During the pandemic, his team has transitioned to working remotely and the firm has decided to keep a long-term distributed workforce. John loves to travel and decides to use this pivot to plan a 6 month road trip where he'll be able to work on the road.

John and his company value security so he outfits his devices with protective security software, makes sure all of his passwords are up to date, and schedules a call with his IT team to make sure he understands the ins and outs of the company's security policies. He's excited to get on the road and feels prepared and protected from the security threats he knows exists.

While traveling, John's security system holds up beautifully - with the exception of a stint in Glacier National Park when he can't find access to a private network. He decides to hop on a public WiFi connection at a local coffee shop, sure that it's a small risk in the scheme of things. While sending a few quick emails, a bad actor infiltrates John's device and installs a version of malware to collect data, credentials, and valuable patient information - in addition to a myriad of John's personal information and access.

Three months later, John's company suffers a huge breach that puts their company and their entire customer base at risk. Security experts trace the breach back to John's session at the coffee shop. They lose a number of clients who no longer trust their technological expertise in the face of such a security faux paus and are forced to lay off a number of team members to address diminished revenue. John is shocked and embarrassed that he's caused such a fuss and resigns from his post leaving the company with a gap in operations talent. Two years after the breach, the company is still dealing with the fallout of this incident on their team and their reputation and John is still recovering from the impact on his personal credit.

EXTRA CURRICULAR READING

Click the titles below for further information from resources we trust.

Cloud security in 2021: A business guide to essential tools and best practices
zdnet.com // 07.22.21

Today's data security RFP must measure what really matters
techhq.com // 06.26.21

Reporting Matters – even for a Smishing Message
staysafeonline.com // 07.20.21

YOU'RE GOING TO WANT TO KEEP THIS PAGE

THE HUMAN FACTOR: BYOD

PLAYBOOK

8 TIPS TO KEEP YOU OUT IN FRONT

CREATE A BYOD POLICY

Many companies don't take the time to create an official policy when it comes to BYOD but doing so can go a long way in getting your employees on the same page security-wise. We'd even recommend taking it one step further and require employees sign an official security policy.

SUPPORT YOUR EMPLOYEES' SECURITY EFFORTS

Provide tools like security software as well as regular tips that your employees can take to increase their personal security - for instance, educate them about the importance of a secure WiFi network.

REQUIRE MULTI-FACTOR AUTHENTICATION ON DEVICES

Multi-factor authentication (or MFA) will add a robust layer of security for your team. In fact, adding MFA can reduce your risk of getting hacked by 99.9%!

EMPLOY A ZERO TRUST POLICY

A good idea even without BYOD, your organization can follow a zero trust policy for your devices and processes and make sure to verify anything and everything trying to connect to your systems.

MONITOR ACCESS POINTS

Even if you've taken the time to set your policy down in writing and communicate with your employees, it's likely they will try to access data with new devices from time to time. Incorporate tools to monitor for new sources of access.

MONITOR FOR NON-COMPLIANCE

You may also want to consider tools that help monitor for non-compliance by your employees. For instance, you'll want to make sure that outdated operating systems are updated before allowing a device access to your data.

CONSIDER CYBER INSURANCE

In addition to creating an official cyber security policy and BYOD regulations, your organization may want to consider adding a cyber insurance policy. Much like a homeowners policy the goal will be to never use your cyber insurance but have it as a backup "just in case."

BE ON CALL FOR LOST DEVICES

With the recovery rate for lost devices clocking in at only 7%, it's imperative for your organization to support employees when the worst happens. Create a system and a triage team that your employees can contact and make sure they have the information and tools they need to do so.

OUT IN FRONT WIN

FIRST EVER CYBER REGULATIONS FOR PIPELINE OPERATIONS

Cyber security issues are not new but we do see a trend of increasing vulnerabilities and widening reach when it comes to attacks. Nevertheless, there are still major gaps in regulations, reporting structure, and federal policies around cyber security. The Colonial Pipeline attack, which occurred in May 2021 has spurred the first of these regulations into action.

Issued in late May by the Department of Homeland Security [DHS], these regulations are the first for the pipeline sector and would require pipeline companies to both keep a cyber security coordinator on call and report any incident to the Cybersecurity and Infrastructure Agency (part of the Department of Homeland Security) within 12 hours. Those companies who do not comply will face escalating fines.

The main benefit of these regulations is in the knowledge that they will provide about the industry as a whole. While we don't expect the regulations to necessarily limit attacks, they will show how widespread the risk is and identify trends within the industry, allowing for improvements and additional policies to be created.

The long term impact of these regulations will take time to assess but they indicate a step in the right direction as we think about overall security policy. Without clarity into the size and scope of the risk, it's difficult to prevent and address those risks. There is much to be learned about how the DHS will evolve these policies but we look forward to improved clarity and collaboration around cyber threats.

We spoke with Mark E. Patterson, EVP Chief Technology Officer of Clark Capital Management Group to get his unique perspective on the recent Colonial Pipeline attack and his organization's approach to security. Clark Capital Management Group is a family and employee-owned investment management firm based in Philadelphia, PA and a client of EMBER IT. Mark serves as their head of technology and is personally focused on keeping the company, employees, and data secure.

ClarkCapital MANAGEMENT GROUP

Q: WHAT DID THE COLONIAL PIPELINE ATTACK MEAN FOR YOUR BUSINESS?

A: When you have incidents like that make the national news and you see the impact, it makes you review your policies and procedures and think about how you're training your employees. We already have in place a pretty robust information security program but these types of events often come down to your team - either not processing things correctly or a phishing event or similar - so we always want to revisit our policies and make sure we're not at risk. You also start thinking about your tools and testing and making sure you have the right tools in place. That all comes more to the forefront when something like this happens.

Q: HOW DO YOU STAY CURRENT ON CYBER TRENDS THAT ARE RELEVANT TO YOUR ORGANIZATION?

A: We contract with different information security professionals that help us to stay up to date on the trends. We also work closely with our inhouse and outside legal and compliance teams on regulatory guidance and issues identified in the industry. Ember helps us with this specifically on the infrastructure side of things. They specifically help us to see trends and topics that are happening across their clients so we're benefiting from that wide knowledge. We also employ third parties to do white hat hacking. They'll do outside penetration tests or internal vulnerability tests that can help us stay up to speed on trends and identify our own gaps.

Q: WHAT ARE YOU KEEPING TOP OF MIND WHEN IT COMES TO CYBER TRENDS?

A: Phishing seems to be the big thing. It's how these companies are getting hacked because the hackers can mock up an email that looks really similar to your internal emails. Phishing is getting more and more sophisticated all the time and hackers are going after specific individuals, which is known as spear phishing.

Q: HOW DO YOU MAKE SURE YOUR TEAM IS PREPARED FOR AND PROTECTED FROM THOSE TYPES OF THREATS?

A: A lot of it is training and communication. We have monthly staff training calls as well as regular updates on security tech tips. I like to share information that I'm gathering so our entire team can stay up to date. It's also about the software and systems that you have in place. We use systems that help to identify emails that are likely to be phishing attempts and block suspicious sites.

Q: HOW DO YOU THINK COMPANIES CAN PAIR AUTOMATED SYSTEMS WITH PERSONAL TOUCHES TO PROTECT THEMSELVES?

A: We don't just rely on automated systems because there has to be a human element. I mentioned that machine learning system which helps us but it still has to be trained and monitored to avoid isolating something when it shouldn't be. We also do require annual training with our employees that helps them see that the threats are real and what they can do about those threats. I also like to bring in subject matter experts to help with specific topics because there's no way we can know everything.

Q: HOW DO SECURITY PARTNERS HELP YOU TO FEEL BETTER PREPARED?

A: What they do is bring best practices to us that they're learning from other clients. I see it as crowdsourcing knowledge and using that knowledge as part of our toolkit. They help us stay current and prepared.

EMBER™

Delivering best-in-class cyber security, IT management, and consulting services to small-to-mid-sized businesses

EMBERIT.COM