




Ransomware Prevention & Remediation

Playbook

AGILEBLUE

AgileBlue, 2022

TABLE OF CONTENTS



02-05

How to Strengthen
your Cybersecurity
Posture

06-07

Tools , SaaS Systems and
Practices to Help Detect
and Prevent Ransomware
Attacks

08-09

Ransomware FAQs
Answered

10-11

Conclusion

12

About AgileBlue

HOW TO STRENGTHEN YOUR CYBERSECURITY POSTURE

With attacks becoming more sophisticated and ransom demands increasing its crucial that companies across all sectors are protecting themselves against these malicious actors. In this guide, AgileBlue will address actions your organization can take to bolster your cybersecurity posture, including:



Methods to prevent a ransomware attack at your organization



Complementary SaaS systems you should adopt



Develop a concise response plan for handling a breach.

Because of the Covid-19 pandemic, 80% of US companies quickly enabled remote working capabilities in a short period. In turn, many companies are unprotected; forcing cybersecurity leaders to adopt a more sophisticated approach to defend against ransomware.



54% of organizations required remote work in response to the Covid-19 pandemic.



80% of businesses hit by a ransomware attack were hit by 2nd attack.



89% of organizations do not have a remediation plan in place.



DEVELOP A STRATEGIC RESPONSE PLAN

In [Red Canary's "State of Incident Response Report: it's time for a confidence boost"](#), it was revealed that 93% of organizations experienced a compromise of data in the past year, while 82% of executive cybersecurity leaders feel their organization remains vulnerable. Create a formal incident response plan in which every employee knows what to do, step-by-step in the instance of a breach. This plan should be a comprehensive guide to understand ransomware damage, back-up processes, and recovery.

HIRE THE RIGHT EXECUTIVES TO LEAD YOUR CYBERSECURITY EFFORTS

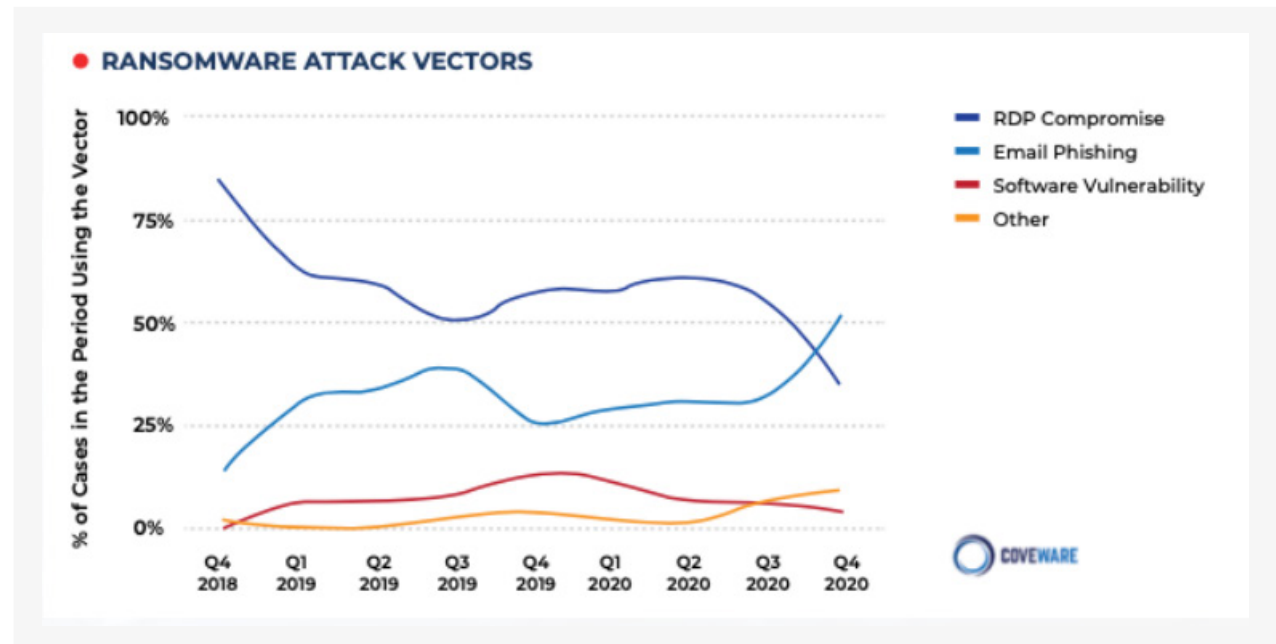
According to a study conducted by [Bitglass](#), 38% of Fortune 500 companies do not have an active CISO. Of those companies who are missing a CISO, only 16% have another executive responsible for cybersecurity within the organization. To develop an in-house team of cybersecurity experts, it takes four SOC analysts at a minimum, plus executive leaders. From time spent on hiring, training, wages, re-hiring, and re-training an individual each time they leave, outsourcing your cybersecurity team becomes financially more responsible.

Making sure a comprehensive plan to respond to incidents is a must, as reports show that one out of two businesses have become compromised in 2020. In 2021 thus far, ransomware attacks have soared as an increasing threat to businesses across the globe.

STRENGTHEN YOUR TEAM THROUGH CYBERSECURITY TRAINING

Training your employees to promote cybersecurity-safe practices in daily operations is critical. In 2020, 90% of data breaches are the result of human error. Yet, 37% of organizations do not have an employee security awareness program in place and 41% of businesses fail to perform compliance audits of partners that store sensitive data.

The visual, provided by [CoveWare](#) to the right represents the most common attack vectors for launching ransomware malware:



In Q4 of 2020, phishing emails surpassed Remote Desktop Protocol (RDP) compromise as the leading attack vector for the year. In fact, [Inspired eLearning](#) revealed that 97% of people cannot detect a sophisticated phishing email – putting confidential business data at risk. By conducting an employee cybersecurity training program, you can mitigate risk of a ransomware attack by 51%.



BACK-UP DATA REGULARLY

Although backing-up sensitive data doesn't prevent an incident from occurring; regularly backing-up data is the easiest way to securely store your data. Paying the ransom is probably the worst strategy to get data back from the hacker, considering only one in every four victims receive full restoration after paying the ransom.

ADD THE RIGHT SAAS SYSTEMS TO YOUR DEFENSE STRATEGY

Make sure you have a next-generation firewall, updated security software installed on all devices, and anti-malware detection paired with advanced end-point protection.

To detect and respond to incidents before you're breached, your business needs the correct tools, so your IT team can effectively respond to any threats across your digital environment and at each end-point.

Obtaining a vigorous and integrated threat intelligence solution is a must to enable your cybersecurity team to detect and respond to escalating alerts. In the next section of this playbook, AgileBlue will breakdown the technology and tools your business needs to prevent becoming the next victim of a ransomware attack.



NEXT-GENERATION SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Rule-based legacy SIEM solutions tend to generate an overwhelming number of false alerts. Nobody likes false positives, they're a waste of both time and money. Consider acquiring a next-generation SIEM platform that collects enormous amounts of data in real-time and actions machine learning to detect local and external threats and provide AI-based incident response capabilities for 0-day threat anomalies.

ADVANCED END-POINT PROTECTION

In addition to 24/7 monitoring, advanced end-point protection solutions use artificial intelligence (AI) to learn new methods of attack and respond immediately. When the threat is identified on an end-point, it's isolated immediately to prevent spread across the digital environment.

NETWORK TRAFFIC ANALYSIS (NTA)

Cybersecurity executives struggle to locate slow, low-sophistication attacks. These unique attack vectors go un-noticed without monitoring system pattern behaviors, network traffic activity, and user actions.

EMAIL CLOUD SECURITY

Traditional SaaS solutions fail to adapt adequately for the cloud. However, cloud-based email security solutions stop threats before they reach the recipients mailbox by monitoring escalations and identify discussions held on the dark web and cybercriminal websites in which attack tools can be purchased. Email cloud security software provides defense against internal threats, business email compromise (BEC), and breached accounts.

DARK WEB MONITORING

The Dark Web monitoring can identify threats or compromised data. Using a monitoring service that pairs your intelligence program to your risk profile, delivers relevant intelligence and recommendations on how to mitigate risk which will increase your protection against phishing emails and ransomware attacks.

WEB SHIELDING

Web applications have security vulnerabilities that can easily be exploited. As attack methods become more sophisticated and applications become outdated, web apps need to be better protected to avoid compromise of data. Web shielding services enables organizations to monitor web apps, meet compliance regulations, and secure your business with the utmost level of security during digital transformation



No matter how prepared you are, a hacker may still find a hole in your security. In the event an attack takes place, what should you do? Below are the most important questions you need to answer after an incident occurs:

WHO DO WE CALL FIRST?

If your organization utilizes a SOC-as-a-Service (SOCaaS) to handle your cybersecurity needs, your cybersecurity experts will likely call you first. Otherwise, your next call will most likely be your general counsel as they know the ins and outs of cybersecurity law. It's important to note that you should file an official report with law enforcement.

WHAT'S THE BEST DISCLOSURE STRATEGY?

When referring to the situation, should you call it a breach? A breach is a legal term that represents a much more severe situation. When disclosing what happened you should refer to the situation as an incident or an event. Your business should develop an appropriate disclosure policy and make it available to the public. This way, ethical hackers and the information security community are aware that your organization is prepared to handle security disclosures. Depending on the industry you're in, you may have laws or other regulations that mandate you report incidents. For example, HIP-PA-compliant organizations are mandated to ensure that all patient health information has strong confidentiality. As an additional precaution, have your Public Relations team ready to handle any crisis communications.



IF WE DECIDE TO PAY THE RANSOM, WILL WE BE SAFE AFTER?

Paying the cyber criminals is, in no-way a plan to receive full data restoration. In fact, 92% of organizations that pay the ransom have not received 100% data restoration. Even if you pay the ransom, you will need to keep guarding your digital environment. However, if you plan to pay the ransom, use a vendor that can make the payment in a legal way. The payer must be included on the approved list from the U.S. Treasury Department and will need to file a Suspicious Activity Report (SAP) to the Financial Crimes Enforcement Network bureau (FinCEN). Also make sure to notify law enforcement once a payment has been made. In the simplest terms, do not pay the ransom.

WILL WE BE FINED?

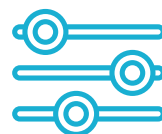
The Treasury Department's Office of Foreign Assets Control (OFAC) already has a list of hacker(s) groups that you cannot pay by law. If you pay a listed terrorist group, you will pay a fine. To avoid this, follow the [FinCEN guidelines](#) for how approved vendors can register and report ransom payments. Individual states have different laws – a state may fine an organization for not reporting an event within a given period of time. In turn, more communication with regulators and law enforcement mitigates the risk of being faced with fines.

CONCLUSION

One of the best ways to mitigate the risk of ransomware attacks is to outsource your cybersecurity defense needs by adopting a Security Operations Center-as-a-Service (SOCaaS) platform, backed by a team of cybersecurity expertise. However, capabilities and service level quality can vary widely between SOCaaS providers. Potential buyers of cybersecurity services should look for SOCaaS providers that can offer the following:



Highly Reliable Anomaly
Detection and Reduced
False Positives



Simplified Setup and
Service Initiation



Robust
Logging



Highly Intuitive
Dashboards Offering Full
Visibility



Correlation-Based
Detection Insights



Highly Responsive
Cybersecurity Specialists

AGILEBLUE

AgileBlue is a software company with innovative SOC|XDR-as-a-Service for 24/7 monitoring, cloud security, data privacy and compliance backed by our U.S. based SOC.

We detect cyber threats before you have been breached. Our SOC-as-a-Service platform is designed to monitor your cloud, network, and endpoints. Our modern SOC-as-a-Service is built on innovative machine learning and autonomous execution. For more information, visit our website: AgileBlue.com.

Ready to start protecting your company?

[Request a Demo](#)