CAPINTECH

# How to Take Your Ransomware Controls to the Next Level

By Allison Davis Ward, Partner

As our article on The Current State of Ransomware notes, ransomware poses significant risks for all organizations of all sizes, and the impact can be long and far-reaching.

Fortunately, there are key controls that can mitigate your organization's risk. We encourage you to consider the following protections.

**Baseline Protections**

Start by reading this article to learn baseline controls to help mitigate your risk of a ransomware attack and what to do if your organization is attacked.

**Evolving Protections**

As we've seen, however, ransomware is becoming increasingly complex, and baseline controls alone may not provide the level of protection you need. That's why it's important to consider evolving protections. Start by performing a risk assessment to see where the biggest threats lie so you can prioritize controls and include your cybersecurity goals and requirements in strategic plans.

The underlying goal of evolving protections should be to increase visibility, adaptability, and response throughout your environment. Legacy tools can be great at identifying things that are known — viruses we've seen before and threats that have occurred in the past. But cyber threats, including ransomware, are constantly evolving. You need tools that can evolve with the threats.

Adaptive security encompasses layered solutions that can provide continuous monitoring of your environment, constant learning from your activity, and anticipation of new threats from analyzing external information and events. When deployed successfully, adaptive security can allow your preventative and detective controls to evolve with the threats in real-time.

Many tools exist to support adaptive security, and new ones are continually being developed. Understanding the main concepts that drive the successful implementation of adaptive security solutions will help your organization select the right tools for your specific environment.

There are four underlying areas to consider when choosing tools to help your organization evolve your control framework and strengthen your defenses against ransomware.

**1. Your tools should learn from behavior.**
Solutions that support adaptive security use technology such as artificial intelligence (AI) and machine learning to analyze behaviors and patterns of activity and learn your normal activity. This allows them to identify known, existing threats as well as suspicious activity that indicates an unknown issue.

These tools can also learn how your organization reacts to certain events and mimic your decision-making to respond to similar patterns or behaviors that occur in the future. They won't eliminate the need for security staff, but they will help you focus on more complex incidents that require a human response by analyzing and responding to the recurring, less severe incidents that often fill up a security team's pipeline.

Two examples of where we will see this more are in email solutions and anti-malware protections. Enhanced email solutions will learn employee's behaviors in the context of what they do and who they interact with and will develop complex filtering based on their normal activity patterns. Similarly, more robust anti-malware

Ransomware is becoming increasingly complex, and baseline controls alone may not provide the level of protection you need. That's why it's important to consider evolving protections.

protections will use AI, machine learning, and behavioral analysis to identify not only known strains of malware but also suspicious activity, such as large volumes of data being encrypted, that may be indicative of new strains of malware.

**2. For extra protection, add in prediction.**
Good cybersecurity includes preventative controls coupled with detection and response, but enhanced tools can also support the concept of prediction. As we noted, organizations can benefit from tools that can learn from the activity happening in their environment. But there are also benefits from learning from real-world events before they happen to you.

Tools that support prediction gather data from events happening all over the world and determine what that means for your environment. This can help you evolve your controls before these events happen in your organization.

**3. Consider tools that support deeper detection.**
Many organizations focus on activity at the perimeter of their network. They have firewalls and intrusion detection systems that help prevent malware and other threats from entering their network. While these controls should be a component of your cyber control framework, there is always the risk that new and evolving threats will find ways into your network. And the standard perimeter security deployed in the past doesn't protect you once the ransomware has entered your network.

Consider adopting tools that allow your organization to monitor and respond to activity throughout your network, not just at the perimeter. The tools should:

- Establish baselines for what your activity looks like on a typical day and identify when something deviates from them
- Monitor standard concerns, such as malware activity and successful/unsuccessful logins, but also look at other data points that can provide insight into unusual activity around changes in files, unusual activity within applications, elevation or escalation of privileges, fluctuations in internal traffic, etc.

For adaptive security to be successful and comprehensive, you need data from multiple points within your network.

**4. Correlation of data is essential.**
The correlation of data will be increasingly important as organizations strive for adaptive security. Without it, an anomaly in one system may not be escalated properly or appear problematic. However, correlating the data being gathered from various points in your network can help your system identify when anomalous activity is indicative of a larger issue, and escalate the alert to allow for a quick and effective response.

These tools also can increase efficiencies as they can work through false positives and present relevant threat information to you on clear dashboards. You can focus on responding to the event, with less time spent gathering data and determining what it means when you look at it all together.

**Next Steps**

Ransomware is not going away. It's critical to start thinking about next steps and how you can better protect your organization and your constituents from the impact of ransomware.

Start by discussing the threat of ransomware, its far-reaching impact, and the necessary controls your management team so they understand the importance of devoting resources devoted to preventing it.

Next, assess how successful your baseline controls are at mitigating the risk of ransomware. If you determine that enhancements are warranted, start considering and planning for solutions that can help you become more adaptable in preventing, detecting, and responding to this issue.

Finally, consider ease of use. You don't want to implement solutions that become so complex that it impacts the effectiveness of your security team. When done right, many of these tools will create efficiencies; however, every organization is not the same, and your needs may differ.

Please contact us at cybersecurity@capincrouse.com with questions or to discuss how CapinTech can help your organization assess and reduce your risk from ransomware and other cybersecurity threats.

**Additional Resources:**

Understanding Ransomware: Malware in Its Cruelest Form

The Current State of Ransomware

The State of Ransomware and Enhanced Controls Recorded Webcast

## About the Author

**Allison Davis Ward, Partner**
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

## About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

## About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

© 2021 Capin Technology LLC