Ransomware Galore: The Four You Shouldn't Ignore

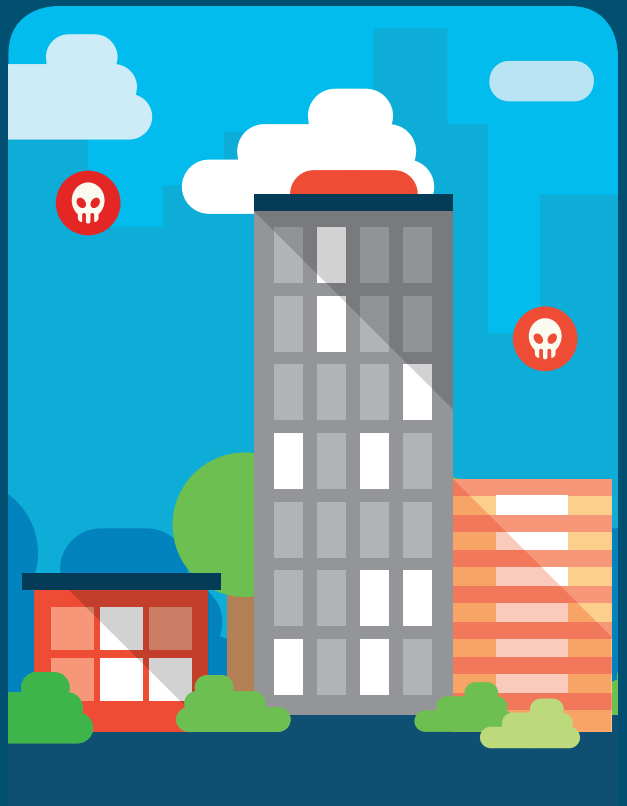
Ransomware. You know the risk is there.

Ransomware is a growing issue that isn't going away anytime soon. The threat of losing access to your mission-critical systems and data can keep you up at night. No one wants to receive a hacker's demand to pay now or lose your information forever.

That's why you've already renewed your focus on data backup and recovery. It's hard, and you know you need to do it. Beyond that, do you know what your top defensive priorities should be?

There are four more things that you absolutely must do.

Let's Explore the Four You Shouldn't Ignore.



The Four You Shouldn't Ignore

DNS-Level Security

Email Security

Malware Protection for Endpoints

Incident Response Plan

Defending against ransomware requires more than just a good backup strategy. You must take key preventative steps, while also readying your team to act when it strikes.

An effective risk-based approach to prevention considers not only the threat but also your vulnerabilities, the likelihood of occurrence, and the severity of impact. You already understand the threat and potential ramifications. How about your vulnerabilities and the chances you'll be affected?

Vulnerable targets exist in every organization. They're your people.

Nearly anyone can be tricked into clicking malicious links or opening harmful email attachments that download ransomware. Then their infected devices spread the ransomware across your network to critical systems. Files are encrypted, systems are slow or offline, and you're presented with a payment demand to get your data back.

This attack method succeeds so often that hackers continually target individuals each day. That's why the chances are very high that someone in your organization will do something soon that elevates your risk of a ransomware infection. If you have people in your organization, then the odds are already stacked against you. You're vulnerable to a ransomware attack.

When ransomware strikes, do you know how long it will take to restore everything from backup? What will you lose by being down for that long?

To restore operations fast, many are tempted to pay the small ransom. Don't.

Stop ransomware before this scenario happens to you. There are many things you can do, but here are four critical steps that address your highest ransomware risks:

Learn more about Cisco Ransomware Defense today at:

www.cisco.com/go/ransomware

The Four You Shouldn't Ignore.

DNS-Level Security

The Internet doesn't work without the Domain Name System (DNS), and neither does most ransomware. Attackers need the flexibility of DNS, which is why ransomware usually doesn't have hard-coded IP addresses. More than 90% of ransomware variants today rely on DNS to remain under the hacker's control.

You already run DNS on your network, so why not use it to run ransomware out of your network?

With DNS-level security you can block access to known-bad domains. That means the end user's system simply can't connect to malicious sites because DNS-level security won't give them bad IP addresses. It's the first line of defense against ransomware, and it's very effective.

That's why you shouldn't ignore DNS-level security.

Cisco Umbrella provides DNS-level security, and is a key component of the Cisco Ransomware Defense solution.

Email Security

Who doesn't use email? There's almost no way to conduct business today without it. Unfortunately email is also the most common entry point for ransomware because hackers can trick people with real-looking (but fake) emails. And those emails are laced with harmful links or attachments.

You can't stop using email, so it's wise to embed email security into your existing email system.

Defend against ransomware by stopping spam and phishing emails. Remove malicious attachments. Users can't click harmful links or open malicious attachments if they don't actually get them. Mitigate email-borne ransomware risks.

That's why you shouldn't ignore email security.

Cisco Email Security with Advanced Malware Protection (AMP) prevents ransomware from arriving through email by stripping away the threat. It's another key part of the Cisco Ransomware Defense solution.

Malware Protection for Endpoints

No matter how hard you try, malware will find a way to reach your users' devices and then spread through your network. People will access bad websites, download harmful files, install fraudulent apps, blindly open attachments, and share infected memory sticks. You can't completely prevent risky cyber behavior, despite all of the security awareness training you've provided.

You need advanced malware protection for all of your endpoints -- user devices and critical servers.

Endpoints are the entry points. They are also the systems holding your critical information. You need a

way to analyze and stop malware from running on those devices and hosts.

That's why you shouldn't ignore malware protection for all of your endpoints.

Cisco AMP for Endpoints delivers essential malware protection for endpoints, and is the third key technology in the layered Cisco Ransomware Defense Solution.

Incident Response Plan

You know the importance of business continuity and disaster recovery planning, which is why you've already bolstered your data backup program. It's difficult and time-consuming, but it's necessary especially considering today's growing ransomware threat.

Of course, you can't begin restoring anything until after you've resolved the cause. Do you know what to do during critical moments after detecting an attack? How will you respond to quickly contain the damage? Without a solid response plan, a ransomware outbreak will cause chaos.

That's why you shouldn't ignore the value of incident response planning.

Cisco Services Incident Response experts can help you develop that response plan, and also deal with active cyberattacks that are causing damage now. We encourage our Incident Response Services to complement the Cisco Ransomware Defense Solution's preventative technologies.

In Line with Cyber Best Practices

The Four Your Shouldn't Ignore were not simply pulled from thin air. They are in line with existing and well-regarded cybersecurity best practices like the Center for Internet Security (CIS) Controls. For example:

CIS Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. DNS-level security provided by Cisco Umbrella is one of many secure configurations that help harden the system and minimize vulnerabilities.

CIS Control 7: Email and Web Protection. Cisco Email Security with AMP is a natural fit with this control.

CIS Control 8: Malware Defenses. Both Cisco AMP for Endpoints and Cisco Email Security with AMP offer the critical malware defenses outlined by this control.

CIS Control 19: Incident Response and Management. Cisco Incident Response Services can help you develop the comprehensive set of people and process controls that CIS recommends. What we call an "Incident Response Plan" is the really same detailed incident response infrastructure discussed in this Control. Plus our Incident Response experts can help you take the necessary corrective action when you're suffering from an active ransomware outbreak or other cyberattack.

More Beyond the Four

Don't stop after you've made progress on the Four. Cisco Ransomware Defense goes a lot further and provides:

Network Segmentation. Logically separate the things on your network that shouldn't be actually talking with one another.

Visibility and Enforcement. Know what's on your network and how they communicate for a clear, consistent access policy.