riskrecon
mastercard

Managing the Risk of Ransomware in the Digital Supply Chain

RiskRecon's Kelly White on Lessons Learned From Destructive Ransomware Incidents

riskrecon
mastercard

Kelly White

Prior to founding RiskRecon, White held various enterprise security roles, including CISO and director of information security for financial services companies. He was also practice manager and senior security consultant for CyberTrust and Ernst & Young.

RiskRecon, a Mastercard company provides cybersecurity risk ratings to enable better third-party security risk management, recently studied the impact of destructive ransomware incidents and the unique tie between ransomware susceptibility and an organization's cybersecurity posture. Kelly White, co-founder and CEO of RiskRecon, discusses the findings and how to use them to help secure the digital supply chain.

In a video interview with Information Security Media Group, White discusses:

- Findings and surprises from the study of destructive ransomware;
- The tie between ransomware susceptibility and cybersecurity posture;
- How to better manage digital supply chain risk.

Destructive Ransomware and Cyber Hygiene

TOM FIELD: You have recently conducted research on destructive ransomware incidents. What did you hope to learn going into this project?

KELLY WHITE: There is surprisingly little data on a large-scale study basis that correlates the risk outcomes organizations are achieving through

maintaining good cybersecurity hygiene. Is it paying off, or is it not? So that's what we were seeking to do: What's the correlation of good cybersecurity hygiene and destructive ransomware event frequency? We picked destructive ransomware as a corpus of study because it is a subset of what is referred to as ransomware. There are at least two broad categories of ransomware attacks. One is the destructive ones that result in system encryption and operational downtime for the company. And the other is data theft, where the data's stolen and the organization is held ransom for not publicly releasing the data.

We are particularly interested in the destructive ransomware because it represents a very significant compromise and a tremendously impactful event to the business. It's shutting down the operations. You have to get an initial compromise vector, and then you have to pivot inside the organization to get to operationally important systems, where you can detonate the ransomware and encrypt the systems to the point that it disrupts operations. So, destructive ransomware provides a very unique lens in studying the effectiveness of good cybersecurity hygiene, or on the other side, poor cybersecurity hygiene. Who are these victims? What's their hygiene? Is it good? Is it bad? Are these investments paying off or not in the form of good risk outcomes?

Research Study Surprises

FIELD: What surprised you from what you learned?

WHITE: What surprised me is: When you go into these studies, you don't know where the data's going to take you. At a certain level, I wanted it to be true that organizations who have good cybersecurity hygiene have lower frequencies of bad or undesirable risk outcomes like destructive ransomware. But I was surprised by just how impactful good cybersecurity hygiene is in reducing the frequency of these destructive ransomware events.

Since 2016, we've identified 1,000 publicly reported ransomware events that were destructive and shut down the operations of the business. That includes hospitals, schools, mining, manufacturing, transportation – things that cannot operate their business or they're operating in a significantly degraded state. Companies that have poor cybersecurity hygiene, according to the study, have a 50 times higher frequency of ransomware

> "Organizations that have poor cybersecurity hygiene have a 50 times higher frequency of ransomware events. That's a big, bold statement, and I can back it up."

events. So it's very obvious in the data that good cybersecurity hygiene pays off, and conversely, poor cybersecurity hygiene sets you up for some undesirable risk outcomes.

We're able to see the cybersecurity hygiene in fairly good detail, at least for the internet-facing systems, on the day of ransomware detonation for all of these organizations, because of the mass-scale cybersecurity ratings and assessments that we do at RiskRecon that give us a lens that we can measure this through.

50 Times Higher Frequency of Ransomware

FIELD: What is the tie between ransomware susceptibility and an organization's cybersecurity posture?

WHITE: Organizations that have poor cybersecurity hygiene have a 50 times higher frequency of ransomware events. That's a big, bold statement, and I can back it up. RiskRecon rates cybersecurity hygiene, continuously monitoring hundreds of thousands of organizations on a scale of A through F, F being the worst. In the D- and F-rated companies, compared to the A-rated companies, is where you see 50 times higher rates of ransomware events. That's based on the state of the cybersecurity hygiene of the internet-facing systems of these ransomware victims on the day of detonation.

Ransomware victims have an 11 times higher count on average of high- and critical-severity software patching issues on their internet-facing systems than the general population. They have a five times higher count on average of unsafe network surfaces than the general population. The same holds true for unsecured RDP, telnet, database listeners on the internet and so forth.

The initial compromise vectors in a destructive ransomware event are pretty evenly split between these three: exploiting an unpatched internet-facing system, exploiting an unsafe network service, and email phishing attacks. So you see a direct correlation between the hygiene that's manifest in the internet presence of these systems and the initial vectors that are used to compromise the organization. Now, that doesn't account for everything, but it's a good portion of it.

As you look at other dimensions, whether it's application security or web encryption, you continue to see poor performance and poor hygiene. Web encryption might not have anything to do with mitigating destructive ransomware events, but these things are indicators of how good an organization is at maintaining good cybersecurity posture in general.

Attacked Organizations One Year Later

FIELD: What is the profile of the types of organizations that are typically attacked, and how do they look a year later? I know you took a look at that as well.

WHITE: The unique thing about this threat is that unlike in the early 2000s where it was all about stealing the data or committing fraud through the systems, it is targeting everyone because the criminals are focused on just disrupting the ability to operate, and they make money by allowing the organization to restore its operations. The 1,000 victims of destructive ransomware are spread across 56 different industry sectors – everything from K-12 education to higher education, local governments and utility companies. Healthcare certainly stands at the top since 2016, representing 17% of all of the destructive ransomware events, but industry sectors like manufacturing account for nearly 10%. So it's hitting a lot of organizations, and every organization's a target if it's dependent operationally on its systems.

What do the organizations look like one year later? The old mythology says the most secure organization is one that was compromised a year ago, because the board of directors and the CEO got their act together. That breach event motivated them to clean things up, make heavy investments and go down the right path. We measure the cybersecurity hygiene of an organization on the day of the destructive ransomware event, and then we look one year later, and we hope to see that those unsafe network services are cleaned up with some good network filtering, that the malicious software that was emanating from their environment is no longer occurring, and software is patched. But it's a mixed story.

One year later, we saw that software patching improved. They have a 36% reduction in the number of high- and critical-severity issues in the internet-facing systems. That's still not as good as the general population, but they're getting there. But unsafe network services exposed to the internet that represent direct compromise are 69% worse. On the day of compromise, the average victim of a destructive ransomware event had 23 unsafe network services exposed to the internet. A year later, the average is 39. They have a 45% reduction in application security issues, but there is a slight degradation in email security. It's not a straight line. So you can't assume that just because an organization suffered a breach that it's going to get its act together and clean things up.

Digital Supply Chain Security

FIELD: What does this all tell you about securing the digital supply chain?

WHITE: This threat is expansive. We saw public reports of 56 different industry sectors that have been targets. Ten years ago, manufacturing wasn't really a target for cybercriminals, but it is now. They represent 10%, and that has significant implications to your supply chain and how you think about third-party risk management. You have to look back at the inherent risk rating model that you're applying to your vendors and ask if you have truly accounted for things beyond data and transaction and reputation risk. Do you have a proper lens on the operational impact to your organization if this vendor suffers a destructive

ransomware event? As organizations do that, they're going to find that there are a number of suppliers that were previously low or moderate risk rated that rise up to the top of importance. You have to solve third-party risk at scale. We had to solve it at scale before, but the threat of disruptive ransomware pushes more suppliers potentially into those high and critical inherent risk tiers. You have even more vendors and a much larger risk surface that you have to manage properly. So organizations will continue to have to manage this risk with limited resources, and from the disadvantage of operating from the outside. You don't have the time or energy or even permissions to look on the inside at the details of every organization. So you have to think about that scale. And where the world has solved things at scale well, whether it's financial risk or legal risk, is through application of data, where you have data that provides you strong correlation and indicators of where your risk is and where there is still risk, but it's much lower.

It's important that organizations get smart about what layers of assessment they're going to put a vendor through. Perhaps once you've gone through inherent risk rating, you apply data to see which suppliers have good cybersecurity hygiene and which ones don't. Then, with that data, you identify those hot spots where you then intelligently engage your risk professionals with those suppliers to dig in deeper and understand what's going on there. Follow the data and the numbers. As you push your suppliers who perform poorly to have better cybersecurity hygiene, and in turn, better security programs, you're going to get better risk outcomes. And with the vendors that are doing well, let them keep going. Concentrate where the risk is.

Focus on Good Cyber Hygiene

FIELD: What's your advice for organizations regarding managing supply chain ransomware risk?

WHITE: Do business with organizations that have good cybersecurity hygiene. If you are accepting the risk of doing business with those that have poor hygiene, you need to go into it with eyes wide open. And you'd better have backup plans and good mitigation plans, both from a data loss perspective and operationally, because those organizations are so dramatically exposed to higher rates of ransomware and data loss events that are going to impact you.

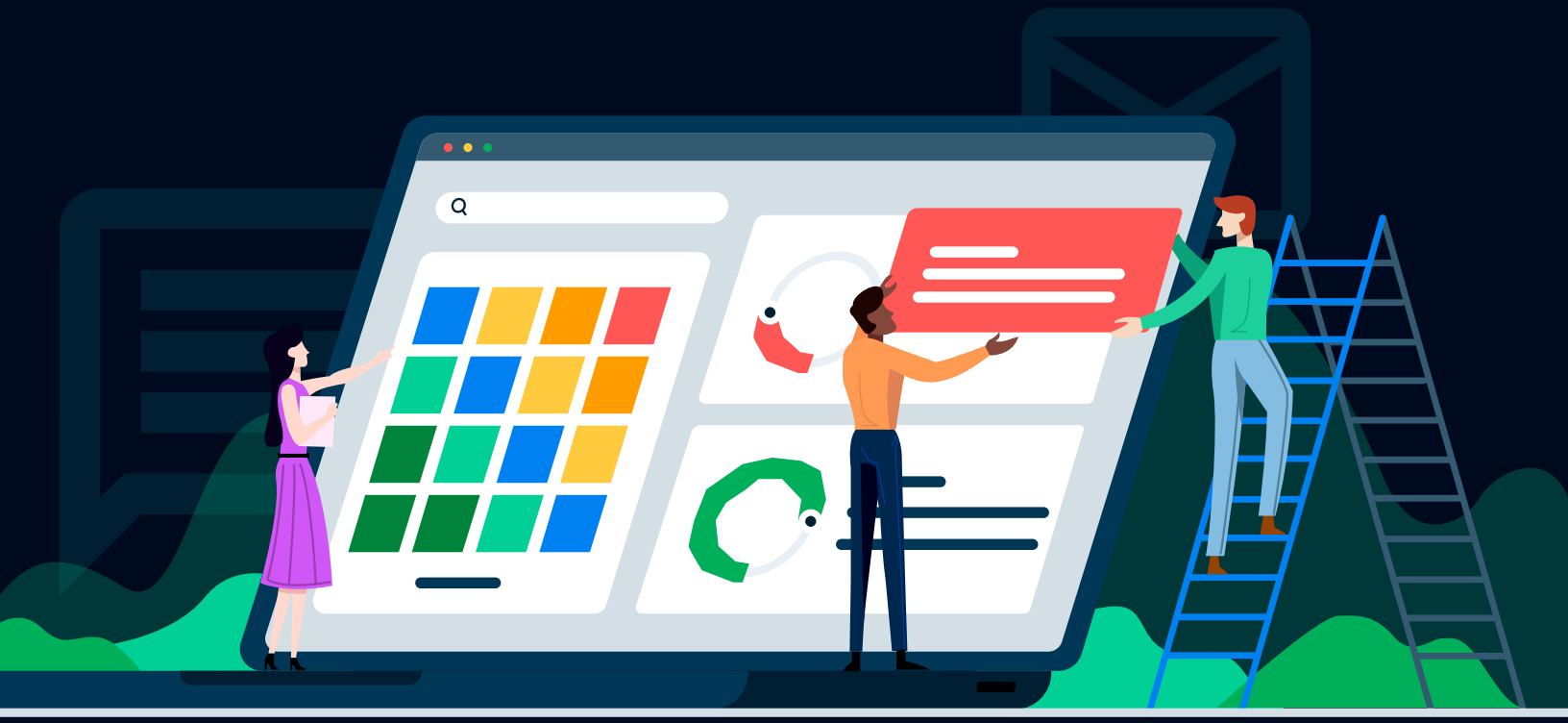
"As you push your suppliers who perform poorly to have better cybersecurity hygiene, and in turn, better security programs, you're going to get better risk outcomes. And with the vendors that are doing well, let them keep going. Concentrate where the risk is."

The RiskRecon Approach

FIELD: Given what you've learned, how is RiskRecon helping its customers to better manage supply chain ransomware risk?

WHITE: RiskRecon, since mid-2015, has been providing cybersecurity ratings and assessments to organizations to shine an objective light onto the cybersecurity hygiene of tens and hundreds of thousands of organizations across the world. This helps our customers understand exactly the cybersecurity hygiene of their suppliers and to take that mass amount of data and narrow it down to the things that represent true risk. Then, our customers can leverage that data to quickly identify who's performing well, who's not, and where they should allocate their resources toward the greatest risk, and in doing so, get the greatest return on their risk investments.

riskrecon
mastercard



Contact us, let's get in touch.

Our solution allows you to instantly identify fourth-party dependencies and concentration risks, as well as every IT configuration and system used by the company.

For general inquiries please contact us at sales@riskrecon.com
For customer support please contact us at support@riskrecon.com