TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

HONDA PLANT SHUTDOWN PROVES WANNACRY RANSOMWARE THREAT CONTINUES!

When a massive cybersecurity threat event like WannaCry ransomware occurs that captures public attention, there is always a larger response from security professionals to stop the bleeding. As such, the fixes come in with exigency in order to protect the global population from the threat. Once there are fixes in place, however, there is an unfortunate tendency for everyday people to think that the threat has been dealt with permanently. I imagine by now that many believe that the WannaCry ransomware threat is a thing of the past, but as a recent breach at Honda proves, this is far from the truth..

September 2017

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

In a report from Reuters, it was detailed how Honda came under attack from the infamous ransomware recently. The Honda Sayama plant, which produces vehicles such as the Accord and Odyssey, was forced to shut down after the WannaCry ransomware began spreading in its internal systems in Japan, North America, Europe, and China. After a four-day period, the plant resumed production following a thorough scrubbing of the ransomware from its systems.

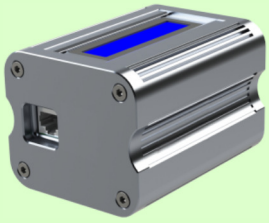
According to Threatpost, it is not clear how Honda went about clearing WannaCry from its network, whether their security division handled it, or they required external assistance. The only statement given about the attack from official Honda sources to media was regarding the production loss in terms of units.

The statement reads:

"A total of approximately 1,000 units were not produced as planned as a result of this interruption. Production has resumed and Honda has taken steps to reinforce its virus protection regimen to avoid any similar occurrences in the future."

The thing is that Honda taking steps to "reinforce its virus protection regimen" is only going to work on the current strain of WannaCry that they faced. Malicious code that accompanies malware is always being improved upon by black hats to cause more damage and penetrate even the most secure of systems. It would be helpful to the InfoSec community if Honda released a threat report about what exactly they faced when WannaCry infected their systems, and how they believe the ransomware entered in the first place.

Latest Network Security Device: "NetDefender"



Vulnerability Management Solution

The new NetDefender Vulnerability Management Solution enhances security by proactively identifying, monitoring, and notifying businesses of potential vulnerabilities in their networks—all with breakthrough simplicity and affordability.

Utilizing proprietary software and the compact NetDefender Sensor, NetDefender works in three phases:

1. Identification

The user's network is continuously scanned to locate and identify every connected device with an IP address, from computers and smartphones to printers and smart devices

Includes scanning of external-facing IPs to provide a 360-degree view of network vulnerabilities

2. Monitoring

All connected devices are then scanned 24x7 for vulnerabilities such as missing software patches

3. Notification

All scan information, including vulnerabilities, is displayed in an easy-to-read dashboard, including instructions for remediation

A proprietary "SPF" (Security Protection Factor) scoring system makes it easy to understand the network's health

Users and their IT security providers can be alerted to critical issues via email or text

For more information on this solution please contact your Tech Hero representative at (800) 900-8234 (option 2)

The moral of the story is that just because the media has stopped reporting on a massive cybersecurity threat, it doesn't mean you are in the clear. Honda learned this the hard way.

Client Spotlight

ORLANDO HEALTH®

As one of the largest tertiary facilities in the region, Orlando Regional Medical Center (ORMC) offers the most advanced care available for all your surgical, medical, rehabilitative and emergency care needs. In addition to a highly qualified team of physicians, nurses and clinical staff, we offer the very latest in technology and diagnostic imaging capabilities. ORMC is a home to Central Florida's only Level One Trauma Center.

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

tech hero

BE PREPARED: HOW TO MANAGE A MAJOR TECH CATASTROPHE

All companies must contend with a crisis at some point in their lifetime. Just look at Facebook when they first implemented their news feed component, or the situation with GE, when they were caught selling weapons to the terrorist-promoting country of Iran. What GE was doing was particularly heinous. Not impressive, Immelt!

We have an idea now on how this crisis can take on many forms – an irate customer, a faulty product, or a critical error on the part of the employee. Unfortunately, too many companies in the United States are ill-equipped to deal with a situation like this due to the absence of a proper contingency plan; according to them, crisis communication plans are more of an option than a necessity.

This can badly damage the business. For a tech company especially, a communication plan is vital for handling a crisis of any scale, and below we take a look at some of the steps a CIO (chief information officer) must take to implement one.

Preparing for all possibilities

It could be that your tech company will never face any large-scale crisis. But you cannot leave anything up to chance. Thus, you should start building a communication plan by first conducting a "vulnerability audit." Speak to all your employees, from the CTO (chief technology officer) to newly recruited developers – ask for their opinion about possible safety measures in case anything goes wrong.

Prepare a list based on their input, and assess how these scenarios might occur. Consider all kinds of possibilities irrespective of the situational details, and prepare talking points.

Springing into action

Build a plan based on the checklist format and have certain protocols in place so that your team understands which steps to follow. They should act fast and keep their wits about them, moving from one task to another with acumen, during what could be a highly emotional period.

As the CIO of a public company, your first task should be to get in touch with shareholders. Based on the magnitude and intensity of the crisis, the press might be on the scene in minutes, and before making any public statements, you must inform the people most affected by the crisis.

If it is an actual emergency, regulatory bodies and law enforcement must be contacted at once. Include your own employees and upper-level management in the response efforts.

Do not commit the mistake of sharing something with the media without first discussing it with your key stakeholders. Use this opportunity to make them see things from your perspective, and provide them with an idea of what to expect. Building a dynamic communication channel will provide you the chance to route the latest details to employees in real-time.

In the event of a major crisis, assurances and explanations need to be provided to the press as well as the general public. The question is, who is going to speak about this? It cannot be handled by just about any random employee; it takes a person who has expertise and skill. Thus, it is important to choose a

spokesperson wisely and clearly. The rest of the committee and board members and employees should assist the media by connecting them to the spokesperson for more details.

The spokesperson for a tech company needs to properly develop their technique for the interview by rehearsing a dynamic opening – one that establishes the company's key messages, and then rehearsing the right way to connect, avoid, and block. It is the responsibility of the CIO to set up a video camera so that the spokesperson is able to practice in privacy. You can even hire a company that specializes in public speaking and interview training for additional support.

Responding to the crisis

The approach adopted by the spokesperson while speaking to the press must be well-planned and executed. For that reason, here are some do's and don'ts:

Areas of focus:

Messaging is key. Apart from the main points highlighting the situation, focus on what the company does well, incorporate the corporate beliefs, values, mission, and commitment into the speech. At the same time, make sure you are completely honest and have a few talking points regarding what the company expects to learn from the situation at hand.

What not to do:

It's always a bad idea to speculate about things. Instead, the best thing is to stick to the facts. If required, you should not hesitate to redirect a question, but make sure you do it respectfully and without offending any reporter.

Stay cool under pressure, and never react to any hearsay and rumors. Focus on the key message and restate the facts. Make it appear to outsiders that everything within the company is under control.

Another thing to avoid is the phrase "no comment." It makes you look like you're guilty and trying to hide something. If you are bound by corporate policy to not answer a particular question – perhaps something to do with private and confidential personnel details – make sure you let the inquirer know clearly.

THE CHANNEL CO.
CRN
MSP 500
2017

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

Why handling a crisis the right way matters:

A botched crisis response may have severe consequences for the company in the long run. It's true that a corporate disaster can affect the company in a bad way, but the importance of healthy relations with the media, both in everyday communications and during the crisis period, prevents things from blowing out of proportion.

Of course, you're free to tell the media nothing. You're not compelled to divulge any details and so you can stay quiet on the matter. But if you think that this is going to make the problem go away, you are sorely mistaken. Maintaining silence breeds distrusts and causes the media to dig deeper into the goings-on in your firm. Moreover, positive media coverage also becomes scarce as a result.

In the event of a crisis, the media will think they lack a cooperative official source, and so they'll approach unofficial sources to get the latest scoop on the crisis. And there's no guarantee that these unofficial sources will present the facts in an accurate manner or deliver the right kind of corporate messaging.

One thing becomes clear in all this – the media must be taken care of and supplied with the kind of information that allows them to do their jobs properly. Present your tech company as a responsive, helpful, transparent, trusted, and solution-oriented entity. Crisis management is a tough call for any company, but having the goodwill of those around you can help you deal with this situation in a more calm and strategic fashion.

tech hero