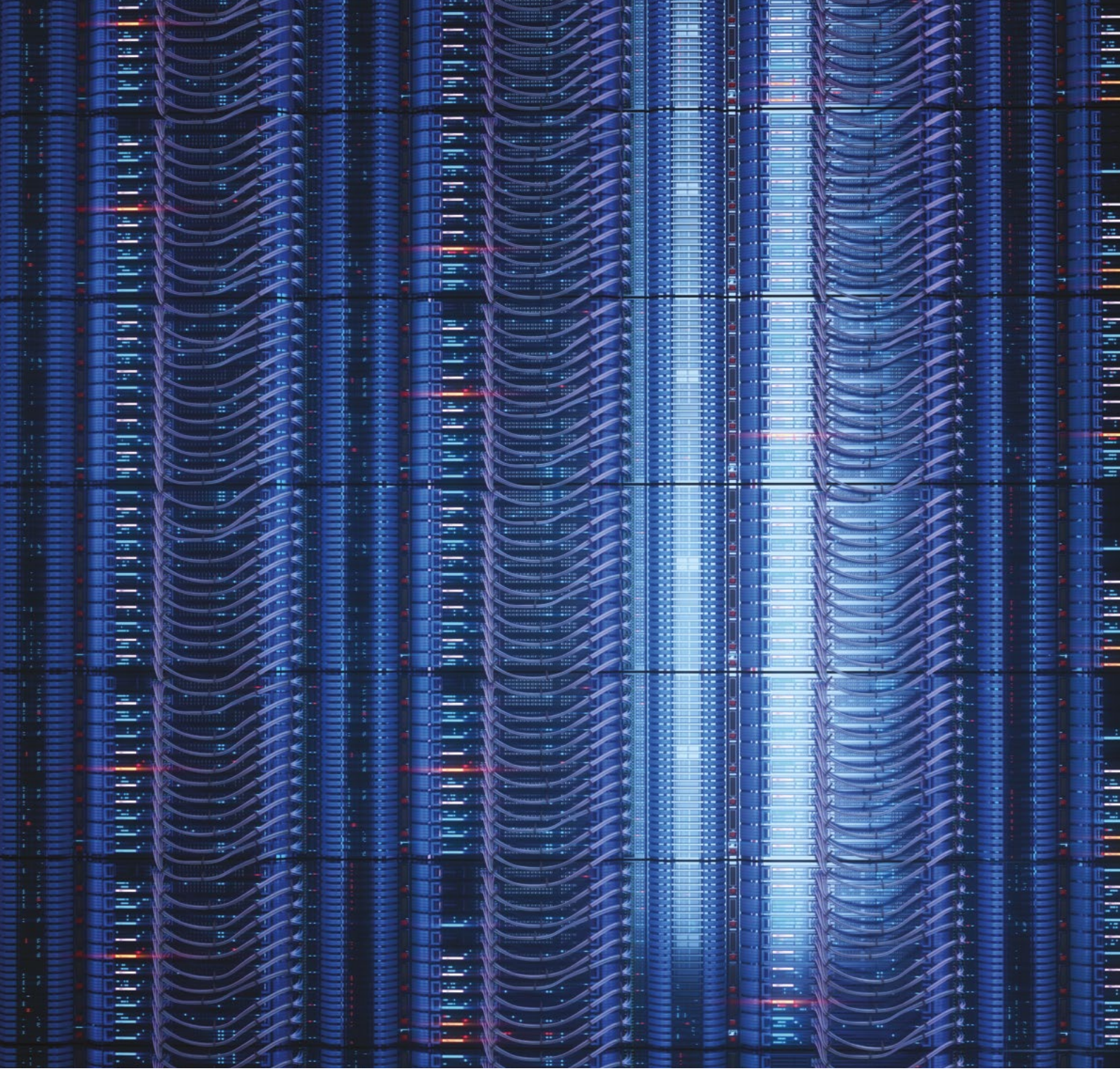


CYBERSECURITY

LIMIT CYBERATTACKS WITH A SYSTEM-WIDE SAFE MODE

Claus Herbolzheimer

Cyberattacks cost companies an estimated half a trillion dollars in damages every year. The main reason they can harm companies to such a staggering degree is that today's cybersecurity systems use centralized monitoring, with little beyond their main firewalls to protect the rest of an organization. As a result, when companies are hacked, it can take days for information technology teams to isolate infected systems, remove malicious code, and restore business continuity. By the time they identify, assess, and resolve the incident, the malicious code has usually proliferated, almost without limit, across any connected or even tangentially related systems, giving hackers even more time to access sensitive data and to cause malfunctions. (See Exhibit 1.)

To stay ahead of new intrusion techniques, companies need to adopt decentralized cybersecurity architectures, armed with intelligent mechanisms that will either automatically disconnect from a breached system or default to a "safe mode" that will enable them to operate at a reduced level until the effects of cyberattacks can be contained and corrected. Like the general security systems at high-risk sites such as nuclear power plants, companies require multiple layers of redundant safety mechanisms and cybernetic control systems. The goal should be to create "air pockets," with neither direct nor indirect internet connections, that can protect critical equipment and internet-connected devices.

Every company's cybersecurity program will have unique attributes, but there are several fundamentals to this decentralized architecture that can help companies shift the balance of power away from the attackers.

DETECTION

Even the most expertly designed cyber architecture is useless if it can't detect and understand the threats it faces. Companies are experiencing more cyber viral outbreaks because they often can't even detect them until it is too late. Today's cybersecurity systems have been built to detect previously identified malicious codes and malware. But cyberattacks are morphing so fast that threat patterns are unpredictable.

To identify and mitigate evolving new attack scenarios, security systems need to search for anomalies, analyze the probability that they are hostile acts, and incorporate them into a continually expanding list of possibilities. This level of detection should be carried out by components on many different levels to cover the multitude of devices and system components connected to the internet and physical environments. Together, these form several layers of cybernetic systems that can identify unknown and new forms of attacks by comparing what they understand to be their normal, uncompromised state – both on their own and in combination with other systems.

Rather than reacting to a defined set of indicators, these systems detect and react to irregularities in data flows, involving anything from the amount, type, origination, or timing of data. For example, to determine whether someone should be locked out of an online bank account, some banks' cybersecurity systems are starting to use artificially intelligent technology to compare how a person normally types or uses their computer mouse.

HARM REDUCTION

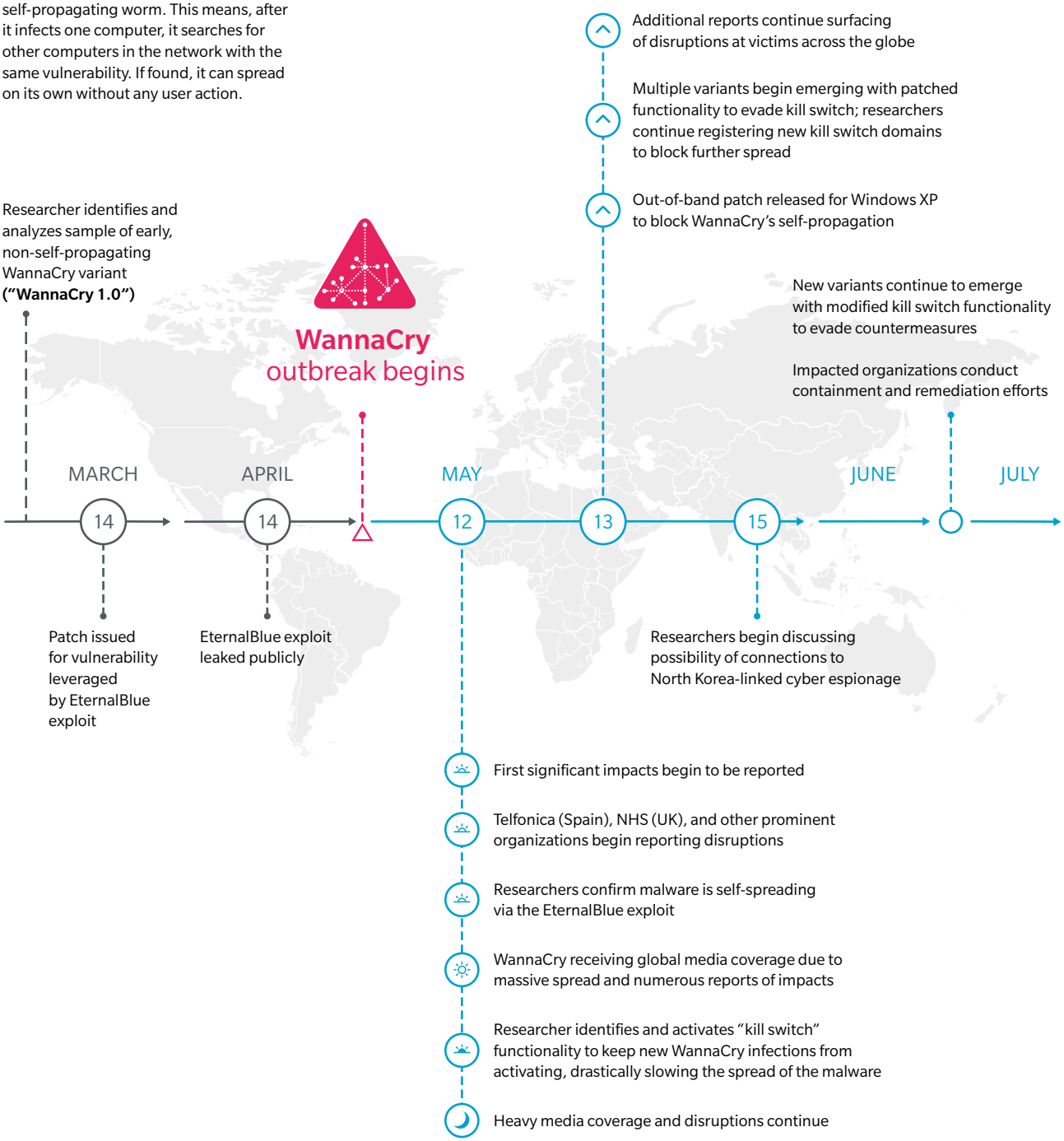
The next step is to make sure that decentralized, intelligent systems minimize the impact of attacks by independently starting a protocol that takes potentially compromised systems offline, disconnects them from other critical equipment, or locks them into a safe mode. Current cybersecurity systems usually trigger an alert if they have identified a specific attack. But they continue to operate and communicate with other systems until information technology teams shut them down and correct the malfunction.

EXHIBIT 1: A MAJOR CYBERATTACK'S TIMELINE

Within three months, WannaCry infected systems in 150 countries

WannaCry 1.0

The WannaCry ransomware is a self-propagating worm. This means, after it infects one computer, it searches for other computers in the network with the same vulnerability. If found, it can spread on its own without any user action.



Source: FireEye

SECURE-BY-DESIGN

Finally, all companies' products will eventually have to become secure-by-design. So far, it seems that companies pay little heed to cybersecurity during product development. That needs to change. Hackers have remotely accessed and controlled everything from network-connected electricity "smart meters," to security cameras. In 2015, Chrysler announced a recall for 1.4 million vehicles after a pair of cybersecurity researchers demonstrated that they could remotely hijack a Jeep's digital systems over the internet. In Germany, nearly one million homes suffered brief internet outages in 2016 after criminals gained access to and remotely shut down their internet routers. The US Food and Drug Administration warns that medical devices connected to hospital networks, other medical devices, and smartphones – such as implantable heart monitors – are now at risk of remote tampering that could deplete devices' batteries or result in inappropriate pacing or shocks.

Companies need to build kill switches, safe modes, and encryptions into their products during development. This will protect not only the companies' systems but also their customers'. Apple, for example, installs layers of data encryption into its products and will permit customers to run only Apple-approved software programs on their devices. Such practices need to become standard operating procedure across all industries.

Stopping cyberattacks will never be cheap or easy. Developing decentralized, intelligent cybersecurity systems will likely happen in fits and starts as devices learn through trial and error not to react to false positives or to go into safe mode more often than is necessary. Managers will have to show leadership, since most customers remain unaware of the extent that cyber risks now pose a threat to the products in their possession, and so are likely to be impatient with glitches and delays.

The good news is that the technology exists to make good cybersecurity a reality. Decentralized, intelligent systems can significantly decrease the risk of cyberattacks and minimize their damage. The savings will be enormous.

Claus Herbolzheimer is a Berlin-based partner in the Digital and Strategic IT practices.

This article first appeared in Harvard Business Review.