On Computer Security Incident Response Teams

Bill Horne | Hewlett-Packard Laboratories

In 1988, Robert Morris, then a first-year graduate student at Cornell University, crafted a clever piece of software that spread from computer to computer. It exploited vulnerabilities in various services to infect machines and spread to other machines while trying to remain covert. This "worm" infected thousands of computers, consuming memory and eventually causing them to become unresponsive.[1] For several days, the community grappled with how to stop the spread of this worm and return systems to normal. Eventually, Morris was convicted under the 1986 Computer Fraud and Abuse Act and sentenced to three years' probation, 400 hours of community service, and fines exceeding US$10,000.[2]

Morris probably didn't intend to cause widespread damage and didn't anticipate the speed at which the worm would spread throughout computer networks. An internal report by Cornell University called Morris's behavior "a juvenile act that ignored the clear potential consequences."[3] This was typical of the threat landscape that unfolded over the next several years: curious hackers who wanted to prove that something could be done without any clear nefarious objective.

What Is a CSIRT?

In response to this event, the CERT Coordination Center, the first computer security incident response team (CSIRT), was created in November 1988 to respond to such security incidents.

Over the next 26 years, systems have become more complex and accessible. Today, cloud computing, mobility, and bring-your-own-device paradigms create significant security challenges.[4] With this evolution in technology there are more opportunities for attack. And because more information that's critical to business operations and our personal lives is coming online, there's a greater incentive for adversaries to try to exploit these systems. The threat landscape has evolved to include much more dangerous adversaries, such as organized criminals, nation-states, and so-called "hacktivists."[5] These adversaries use incredibly sophisticated techniques to find and exploit system vulnerabilities.[6]

In tandem, CSIRTs have evolved from loosely organized groups of system administrators to highly trained organizations with diverse capabilities, relying on complex technology to track, analyze, manage, and remediate security incidents.

CSIRTs can take many forms, but often consist of

- a security operations center (SOC), where security analysts pore over thousands of events each day to determine whether they're attacks or false positives;
- an incident response team that determines how to respond to breaches;
- forensic investigators who try to understand how something happened and collect evidence for potential legal action; and
- an engineering team to develop and maintain complex specialized technologies to support the organization.

> **"I believe that all security professionals can benefit from having a better understanding of CSIRTs, and CSIRTs can benefit from the diverse knowledge and experiences of other parts of the security community."**

For many organizations, the CSIRT is the front line of security defenses—where they determine if they're being attacked and how to respond. CSIRTs are highly labor intensive; it's not unusual for the CSIRT of a large organization to consist of more than 50 people. Labor is the most expensive component, generally far exceeding the costs of the technology components. As a result, organizations are under tremendous pressure to optimize this precious resource.

Yet, as important a role as it plays, many security professionals are completely unaware of what exactly happens in a CSIRT. This isn't surprising as security is a remarkably diverse discipline. Practitioners who deal with the details of operational security are typically unaware of the mathematical theory behind cryptography; cryptographers are typically unaware of the techniques involved in exploiting a vulnerability in a piece of commercial software; hackers are typically unaware of the nuanced legal arguments behind organizations' and governments' policy decisions; and so on. Security is simply too complex an endeavor for a security professional to understand every aspect.

Indeed, when I first arrived at Hewlett-Packard, CSIRTs were somewhat a mystery to me. But I've been fortunate to be involved in many projects over the years that have given me an inside look at exactly what happens in these organizations. I believe that all security professionals can benefit from having a better understanding of CSIRTs, and CSIRTs can benefit from the diverse knowledge and experiences of other parts of the security community.

My goals for this special issue are to educate readers about SOCs and CSIRTs, explore some challenges these organizations face, and describe the state of the art for how those challenges are being addressed today.

In This Issue

The first article, Robin Ruefle and her colleagues' "Computer Security Incident Response Team Development and Evolution," is an excellent introduction to what CSIRTs are, what services they provide, and how CSIRTs have evolved since the first CSIRT was created in response to the Morris worm. If you're unfamiliar with CSIRTs, this is a great place to start.

Next, "A Dutch Approach to Cybersecurity through Participation," by Kas Clark and his colleagues, provides an international perspective describing how the Dutch National Cyber Security Centre operates and how it coordinates with other national CSIRTs, especially those in Europe. It gives an interesting perspective on how a country's culture can influence CSIRT operation.

The next two articles focus on CSIRT technologies. Today, SOCs handle millions—if not billions—of events every day, requiring sophisticated tools to manage this volume of data. In "The Operational Role of Security Information and Event Management Systems," by Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot, we learn about security information and event management systems and the challenges organizations face with event processing.

Our adversaries are amazingly coordinated. They do a far better job sharing information than we do. It's becoming clear that the good guys need to find ways to share actionable information in real time to counter this threat. In "Security Automation and Threat Information-Sharing Options," by Panos Kampanakis, we learn about the alphabet soup of emerging security information-sharing standards.

In "An Anthropological Approach to Studying CSIRTs," Sathya Chandran Sundaramurthy and his colleagues take an ethnographic approach by embedding one of their researchers in a CSIRT to learn what really goes on and posit ways traditional cybersecurity researchers can improve SOCs and CSIRTs.

Finally, we get an organizational psychologist's view in "An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams," in which Tiffani R. Chen and her colleagues give us a deeper understanding of CSIRT job requirements and develop a set of recommendations to help individuals, teams, and multiteam systems collaborate more effectively.

This special issue will give you a greater understanding of what CSIRTs are and how they work. For the security researcher, these articles highlight challenges faced by operational security, presenting opportunities for new research avenues. Security practitioners can use the diverse perspectives presented in these articles to help them be more effective at their jobs. And policy makers can gain insights into how their work might impact these critical organizations. ■

References

1. H. Orman, "The Morris Worm: A Fifteen-Year Perspective," *IEEE Security & Privacy*, vol. 1, no. 5, 2003, pp. 35–43.
2. *United States v. Robert Tappan Morris*, US Court of Appeals for the Second Circuit, *Federal Reporter*, 2nd Series, vol. 928, 1991, p. 504.
3. T. Eisenberg et al., "The Cornell Commission: On Morris and the Worm," *Comm. ACM*, vol. 32, no. 50, 1989, pp. 706–709.
4. N. Perroth, "Security Needs Evolve as Computing Leaves the Office," *New York Times*, 11 June 2014.
5. D.E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, 2001, pp. 239–288.
6. *APT1: Exposing One of China's Cyber Espionage Units*, tech. report, Mandiant, 2013; http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Bill Horne is a senior research manager at Hewlett-Packard Laboratories. Contact him at william.horne@hp.com.