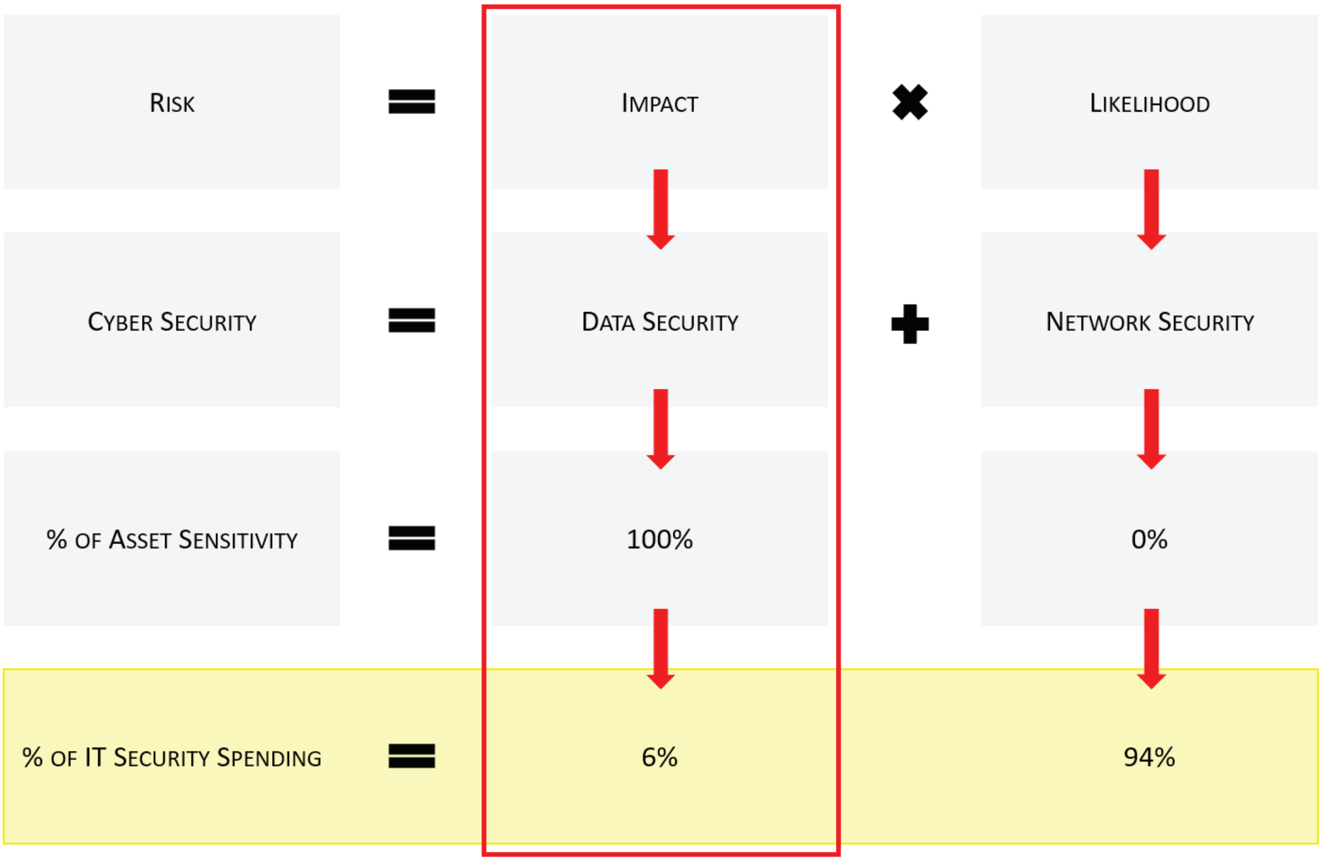
InfoGPS
NETWORKS, INC.

Network security only half of the true cybersecurity story

By Paul Hugenberg

Companies in almost every industry are spending a sizeable percentage of their IT budgets on tools to improve security and reduce the risk of a specific threat from disrupting their business or even stealing their data. Much of this money is focused on building best-of-breed network security perimeter defenses to defend their data.

Unfortunately, as we have seen in highly publicized breaches in the last two years, these incredibly defended perimeters are not enough. In fact, network security spending is particularly effective in reducing the likelihood of certain events, but has little success in reducing their impact. Only data security can mitigate the impact of a breach.



Risk	=	Impact	×	Likelihood
Cyber Security	=	Data Security	+	Network Security
% of Asset Sensitivity	=	100%		0%
% of IT Security Spending	=	6%		94%

Spending only six percent of IT security on critical assets leaves an organization at risk for a significant data breach.

Contrary to public perception, breaches do not happen with the speed of lightning. Even those who attack our networks to disrupt or steal our information have to spend time finding the assets. It takes time, sometimes, a long time. When you are targeted, the bad actor patiently goes through the process of examining your network. This "footprinting" effort is easy and requires little skill. It is also mostly transparent to existing tools. The result is it obtains just enough information to help the attacker determine what tools are necessary to go further. As he discovers what type of perimeter protection system you use, he runs back to his tool box to grab that perimeter system's keys. Once he reaches the next layer, he goes for the tool that works now – and so on, until at last, he finds a way in! A Trojan horse at its most basic definition: a threat hidden inside something that does not concern your controls is allowed inside. Your network has just been breached.

Immediately, the criminal, or criminals, will find a way to obtain administrative rights. They then spend weeks and months sifting through your data, installing malware, reviewing behavior and monitoring your network to find the location of specific information that will become their target. They gather that data, bit by bit, record by record, until they exfiltrate that data back through the very perimeter they came through in the first place! The tools they used to enter without alerting you are used once more to leave.

How are they able to move about undetected looking at every file, every record and NOT get noticed? What are they looking for? How do they find it? How can you prevent it from being detected?

The first surprise is that bad actors residing in your system are most likely NOT in your core system or on your production servers. They are on the other devices in unstructured data repositories. Only 20 percent of your data is in your core. Attackers know that and focus on the 80 percent just outside the view of your existing controls. Nearly every breach that we have heard about (Target, Ashley Madison, Office of Personnel Management Sony etc.) happened outside of the business core. These companies lost data that they did not know they had from places on their network that they did not know the data resided.

We firmly believe no one loses data they know exists. Your IT team is expert at protecting it and your business operating systems. When they have the information they need to protect you, they do a fantastic job. It is the data they don't know they need to protect that becomes the issue!

Revisiting the title of this article, "network security is only half of the true cybersecurity story," we recognize that the missing component, the second half, is data security. Data security is only possible when you know where your critical data is stored.

This final formula presents us with a framework that can be used to discover our critical information, classify it based on its sensitivity, and ultimately apply proper controls around it to prevent unwanted risks. ■

Cybersecurity = Network Security PLUS Data Security.

Paul Hugenberg is CEO of InfoGPS Networks, Inc. Its team identifies, classifies and tracks sensitive data so organizations can secure it and manage its risk across their enterprise systems. Reach him at paul.hugenberg@infogpsnetworks.com. Learn more at infogpsnetworks.com.

Look for additional features about data security for veterinary clinics and the supply chain in upcoming issues of the Animal Health Digest Bulletin.