Jeff Hussey
CEO
TEMPERED NETWORKS

Jeff Hussey is a seasoned leader in the networking and security markets, having founded F5 Networks and led its IPO, the most successful in the Northwest and 17th-best overall in 1999.

FOR MORE INFORMATION:
please visit
www.temperednetworks.com

Securing the Internet of Important Things

Mitigating and managing the risk from constant connectivity

Today, big data analytics and the Internet of Things—which together are known as the Industrial Internet—are creating huge opportunities as they converge onto IP networks. Extracting the maximum value from these connected assets while simultaneously controlling risk is key to success. Current security approaches, though, cannot and will not scale to support the expectations of the Industrial Internet. Tempered Networks CEO Jeff Hussey discusses how organizations can balance connectivity and security while effectively managing risk—to fully maximize connectivity and collaboration in this exciting new era.

With so many touchpoints today, what challenges do companies face in securing them?

We often ask our clients what is more important to them: connectivity or security. Their answer is typically "both," especially in today's world, where machine-to-machine communication is a necessity. In the past, these device networks were often protected by an air gap or little-known communication protocols that provided security via obscurity. But given the connectivity requirements of the modern industrial enterprise, those are no longer valid approaches.

The culprit isn't always bad systems or designs but human error. Why is that?

Our mantra here is that security isn't as much a technology problem as it is a personnel problem. The personnel problem is partly a corporate culture issue, but it is also a function of the complex nature of networks today. The key for any organization is to automate as much of its security as possible while minimizing complexity to reduce human error. But things happen, whether accidental or malicious, so Tempered Networks' mission is to help CISOs minimize their organization's risk profile. CISOs clearly see this as a high priority but struggle with how to counter the huge momentum that comes with the converged industrial enterprise.

How can companies assign a dollar value to breach consequences?

Here's an analogy that works: An organization's board of directors, CIO and CISO need to think about IT security and risk the same way finance professionals do. When traders on Wall Street put through a trade, they know exactly what their risk levels are in terms of dollars. They know that if they are wrong, they will lose X amount of money. The same mentality needs to become prevalent within IT. If your organization is hacked, you are going to lose X amount of money each time. IT professionals need to be able to start thinking like this to properly value, manage and mitigate security risks.

> "Security is complex and expensive in both technical and human resources."

How can companies best position themselves today to both maximize security and minimize the cost of breaches?

Security is complex and expensive in both technical and human resources. So the best thing for any organization to do is ensure that it has thought through the consequences of a security breach and how those consequences can affect the business—in real dollars. With those real dollar values in mind, companies can then begin to compare the investment dollars and value of solutions—such as the ones we offer at Tempered Networks—with the large costs associated with a security breach. ■

TEMPERED NETWORKS™
Hardened. Resilient. Simple.™

IDG
INTERNATIONAL DATA GROUP