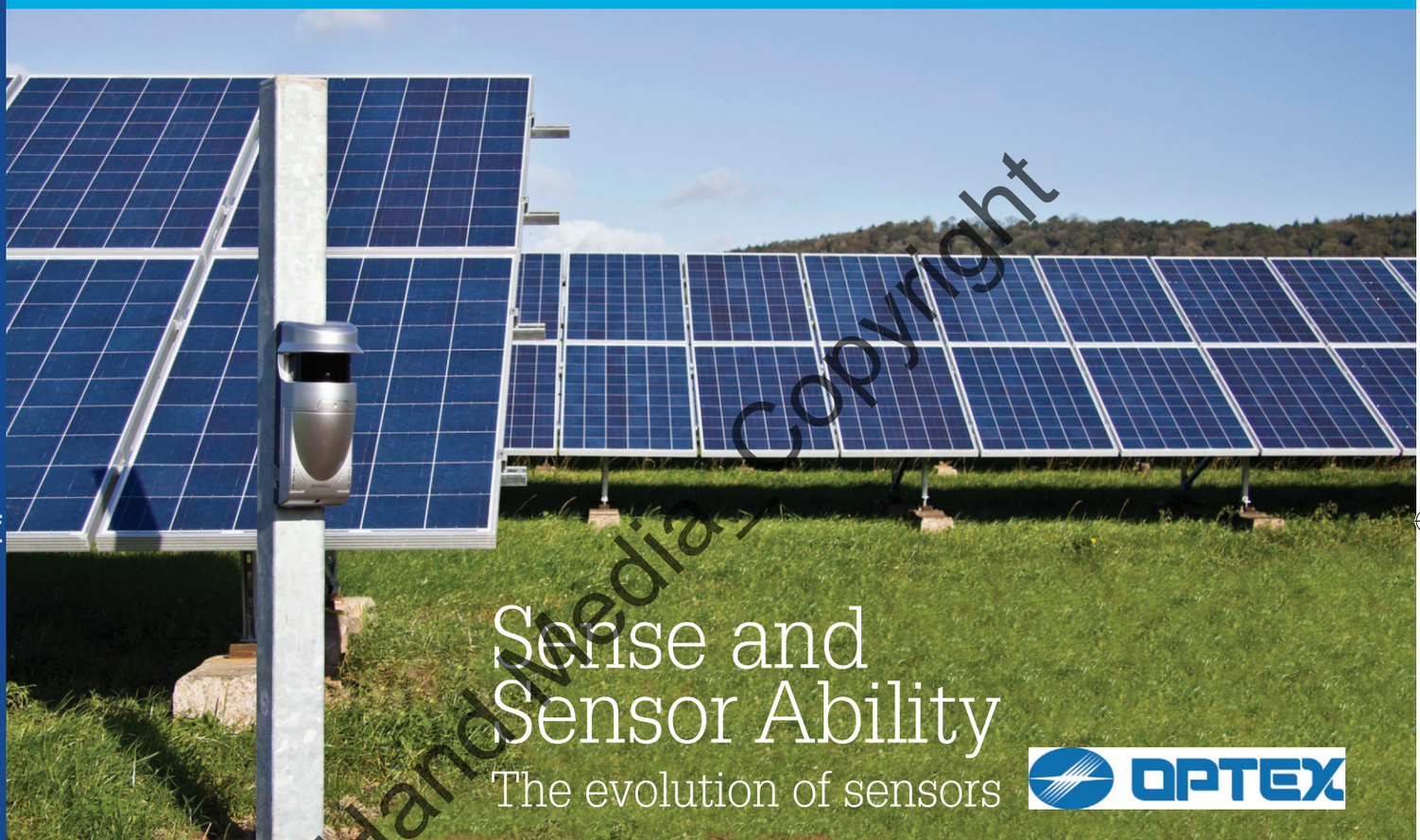
Volume 24 Edition 6 October/November 2016

SECURITY BUYER

FOR TODAY'S SECURITY PROFESSIONAL

www.securitybuyer.com



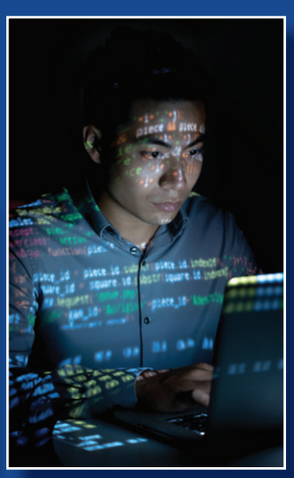
www.securitybuyer.com

THE INDUSTRY'S LEADING SOURCE OF COMMENT, ANALYSIS AND OPINION

UPGRADED SECURITY
HIKVISION'S VIDEO SURVEILLANCE RENOVATION

STUDIO CITY
LARGEST HD CASINO VIDEO SYSTEM IN THE WORLD

BANKING
CYBER ATTACKS: BANKING AT THE FRONTLINES?



HUMBLE BEGINNINGS
A BRIEF HISTORY OF SIEM AND INTELLIGENT SECURITY

Keeping stored data safe and secure

Richard Austin, SNIA Security Technical Work Group member, speaks to Security Buyer about how understanding the modern security 'condition' can keep data safe

Security is an often-discussed word these days and almost everyone agrees that having more of it is better, as if one could walk into the nearest consultancy and say 'I'd like 3 tons of security please.'

The problem is that security is not really a thing at all, but rather a sort of condition.

This 'secure' condition can be said to exist when all the risks an organisation faces are managed down to its risk tolerance at some point in time.

"There are a lot of odd words in that last sentence: 'Risk', 'management' and 'risk tolerance,' and it turns out that most of the confusion about this thing called 'security' is based on a lack of understanding of those terms..."

There are a lot of odd words in that last sentence: 'Risk', 'management' and 'risk tolerance,' and it turns out that most of the confusion about this thing called 'security' is based on a lack of understanding of those terms.

We all have an idea of what risk is - we may have a car accident on the way to work this morning, it may rain today, the stock market may move in an unexpected direction, our business competitor may introduce a significant new product. Each of those possible situations has some things in common:

- There is a particular potential loss (we may be injured in a car accident; we may get wet unless we carry an umbrella ...).
- There is something that can be done to reduce the loss (carry an umbrella, maintain car insurance and drive carefully, diversify the stock portfolio ...)
- There is a general idea of how likely the loss is (40% chance of rain today).

We could put those three factors together into a sort of equation that says that risk is determined by the likelihood of the loss and the size of the loss reduced by whatever we put in place to mitigate the risk.

"Threats make use of and exploit vulnerabilities ('weakness of an asset or control that can be exploited by a threat', ISO/IEC 27032)...."

Risk = f (Loss, Likelihood) – Mitigations

As you apply more mitigations, risk will decrease, so how do you know when you're done? Organisations have a tolerance for risk that varies – some are very conservative and have a very low tolerance for risk. Some, for example a dynamic start-up, have much higher tolerances. You are finished mitigating risks when the remaining risk is within the tolerance of your organisation (or you run out of budget, whichever comes first).

A cautionary note: The information security industry today spends a lot of time talking about compliance, which basically means verifiably doing what some (hopefully) knowledgeable and responsible body has decided is necessary. For example, if you process payment card information, you must comply with the PCI-DSS requirements, or if you store or process personal health information in the USA, you must comply with HIPAA, and the list goes on.

However, 'security' is a different thing than 'compliance.' Compliance basically means that you have followed all the applicable items on some checklist while security implies that all the important risks in your environment have been mitigated to an acceptable level.

Risk management is basically concerned with assuring that an organisation identifies the risks in its environment and mitigates them as much as possible. In an ideal world, there would be a risk assessment, which produced an ordered list of risks, highest to lowest, and we would manage those risks by applying controls (mitigations).

For example, we might purchase and install a firewall to limit the types of traffic incoming to our corporate web servers; or perhaps buy an e-mail gateway that could scan all the e-mails coming into our domain for malware and so on. These mitigations have costs both in acquiring them and operating them and our budget, supply of qualified people, etc., will always be limited so it's important that we apply mitigations where they will produce the greatest reductions in risk for our organisation.

Risk is very much dependent on the particular organisation and its circumstances so it's not really possible to talk about specific risks in a general way. The things that give rise to risk can be discussed much more generally so let's take a closer look at the things which may give risk to risk in our particular environment.

Threats make use of and exploit vulnerabilities ('weakness of an asset or control that can be exploited by a threat', ISO/IEC 27032). Examples of vulnerabilities are the ever-present software defects that keep our patch teams busy or a careless employee who carelessly clicks on a link in a suspicious email.

Successful exploitation of a vulnerability causes an event ('identified occurrence of a system or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant', ISO/IEC 27000) which may have consequences that interest us.

Another useful concept when thinking about threat agents and vulnerabilities is threat vector (ISO refers to this as an attack vector or a 'path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome,' ISO/IEC 27032). A threat vector is the line that connects a threat agent to the vulnerability. In the email example it is this email which is the threat vector.

If the consequence is significant enough, it may give rise to a security incident ('single or series of unwanted information security events that have a significant probability of compromising business operations or threatening information security,' ISO/IEC 27000). An incident indicates that the adversary likely has achieved their objective in penetrating our defences.

Though the terms may seem foreign and somewhat cryptic, they embody an approach to estimating the likelihood and magnitude of a loss. Likelihood depends on threats and vulnerabilities (and how easily a threat may exploit a vulnerability) while consequences measure the loss. Storage management is quite powerful and also fairly exposed as it must be accessible to those charged with managing the storage infrastructure (whether present locally or remotely), vendor support personnel (usually remote) and auditors.

Couple this with the common practice of out-of-band management over a TCP/IP network and it becomes an attractive target for adversaries. And, if there is one area where our adversaries excel, it's in mounting attacks across TCP/IP networks. ISO/IEC 27040 provides solid guidance in securing storage management.

www.snia.org/security

"Though the terms may seem foreign and somewhat cryptic, they embody an approach to estimating the likelihood and magnitude of a loss..."

Richard Austin, SNIA Security Technical Work Group member