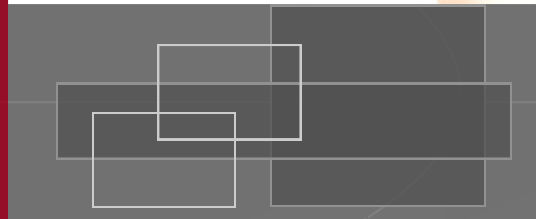
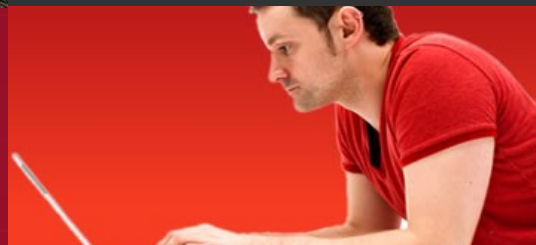


Redefining System Integration:

The re-emergence of humans in corporate security planning



The security industry is an industry in transition. In the seventies and eighties, locks and alarm systems built around standalone technology were predominant. The emphasis in the reseller market was on hardware size and functionality.

In the nineties, video technology and software development began to dominate the industry. Well-positioned cameras and carefully programmed card readers raised the expectations of commercial buyers, facility managers and IT directors. The automated access industry enjoyed double digit growth on the backs of these two, overlapping waves of 'security innovation.'

However, the components in these legacy systems weren't always communicating with each other, creating easily exploited **gaps**. Near the late nineties, the security industry discovered 'system integration.' Pulling all security data together ('interoperability') using LAN servers for easier sharing and detection became the 'holy grail.'

As the Internet matured, it became obvious that security officers could use the IP platform to monitor activity enterprise-wide. Remote monitoring and wireless connectivity are now on the table in the boardroom, especially as the value of intellectual property and digital assets have become better understood.

At this pivotal moment, system integration must be re-thought to fully protect corporations, their culture and their future. Something is still missing...

New ideas on this page:

Tech-trends have taken us from hardware to software to IP platform

Remote monitoring and central data interpretation are the next opportunity

However, there is a gap in the security industry

This is a pivotal moment

The whole concept of system integration must be reconsidered

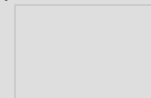
The term 'systems integration' is steadily giving way to 'convergence' as security executives focus on linking together the physical and logical arenas of protection.

The emergence of biometrics and central station data management demonstrate this trend. The industry focuses first on increasing the *effectiveness* of software, then veers toward increasing the *efficiency* of the system of converged components. It's a process that has accelerated for nearly a decade as more and more IT solutions compete for a share of the commercial security budget.

As the speed of transmission on the web increases, more companies are migrating their security programs into the world of Internet-protocol (IP). This allows corporate security directors to monitor multiple locations, cutting costs and speeding response times.

An exciting aspect of these 'converged' security systems is the ability to measure the degree of vulnerability precisely. That information can then be shared with corporate officers for rapid, well reasoned decision making.

In the rush to adopt the latest technology, the human resources department has largely been excluded. Their insight into humans has been dismissed as irrelevant. However, true system integration may not actually be possible without revisiting this assumption...



New ideas on this page:

Despite much progress, system integrators have overlooked a key factor

The convergence of physical and logical security is the next wave

Measuring and sharing vulnerability can prevent breach

HR is on the outside

New ideas on this page:

Human creativity can outwit security programmers

Users of security equipment are behind the curve

Office security procedures are a problem for today's employee

People must play a larger role in security planning

As security technology becomes more vigilant and connected, IT integrators may have overlooked a key element in their effort to protect and preserve: *The very human beings that evade their technology have evolved as well.* Those who represent a threat are more creative than ever. Their willingness to be illogical and unpredictable in order to elude the rational/practical software developer is a growing threat.

Employees, on the other hand, are less tech-savvy than IT staffers anticipate. Often, office personnel responsible for monitoring daily activity never master the less-than-intuitive interface. As a result, training costs and help-desk costs skyrocket, especially when an IT executive adds yet another feature.

Today's employee is more protective of their personal space and their daily ritual in ways that may or may not be 'safe.' Their tolerance for awkward security procedures is less than the software developers originally supposed.

Security guards are numb with boredom as they watch video monitors endlessly. The designers of those displays haven't considered the impact their equipment has on the psyche of its users. Yet without deep, sustained attention (which is nearly impossible), ground-level security personnel cannot be effective, despite their sophisticated IT 'tools.'

People are the **X factor** for security integrators.

IT security engineers, as a rule, forget about people's built-in limitations. They assume that we know our own minds perfectly, can compute everything, compare our options and always choose the best and most appropriate course of action – even under stress. They assume that we are like Star Trek's hyper-rational Mr. Spock.

But, what if employees are limited in the way we use and understand security information? What if we are more like the emotional, biased, fallible Homer Simpson than like Mr. Spock? This may seem depressing, but if we understand our limitations and take them into account, it may be possible to design a better security program, starting with improved interfaces and data interpretation tools.

Security system programmers often display a mixture of naivete and arrogance. When confronted with humanity's flaws and quirks, they simply shrug, even when the costs in extra training, sluggish response and cultural backlash are spelled out. But it's not that difficult to take human capabilities and weaknesses into account. A different approach to selecting and organizing the components in a security program would be to bring real, flesh-and-blood people into the process earlier. This approach would enable security recommendations to achieve their full potential.

New ideas on this page:

The assumptions of tech programmers

Mr. Spock or Homer Simpson?

Sensitivity to employee learning styles

Emergence of HR staff in security planning

Today's new-era security consultants must understand what people can and cannot do; thus, they organize monitors, cameras, computers, alarms, barriers, locks, cables and credentials into a system that can be **used by all**, not just a few. Security planning is becoming an 'egalitarian' process that requires a designer's mindset.

Why? Because understanding people is more like connecting the dots than doing a linear math formula. It requires a feel for motivation, culture and thinking styles, which is why HR staff should be involved at the beginning of security planning.

Any security program that puts people on the same plane as technology requires an emphasis on an intuitive IT interface. Today's employees have been 'spoiled' by the elegant simplicity of Apple's graphical, minimalistic button design and placement. IT executives and security trainers must see this as the big issue that it is rather than regarding it as cosmetic frosting on the cake.

Finally, we need a better approach toward interpreting all this information; something as simple as a custom, graphical user interface (GUI) would help. Even quick browser access (from any PC) could help us transition away from merely monitoring and archiving information to: 1) measuring, 2) comparing and 3) anticipating.

These cognitive strategies deepen our *awareness* and *vigilance*, two human qualities that can **change the 'game' of security-based system integration.**

New ideas on this page:

People are as important as technology.

Security planning requires 'connecting the dots'

A more intuitive user interface will improve employee participation

Better graphics can deepen engagement and prevent breach