



Information security technologies as a commodity input

Information
security
technologies

Andrew Stewart

Consultant, Atlanta, Georgia, USA

5

Abstract

Purpose – The paper provides a pragmatic evaluation of the value that security technologies deliver to businesses. It contains recommendations for how businesses can best view the role of security technologies within an information security program.

Design/methodology/approach – The findings in the paper are derived from the observations of the author in his role as an information security consultant working for businesses in numerous vertical markets over the period of the last several years.

Findings – The principle finding in the paper is that the market for information security technologies is becoming a commodity market. This change will create a shift in how businesses view security technologies, as they will begin to focus on achieving security capabilities at the lowest possible cost. The processes of commoditization will also force security vendors to find new ways of doing business.

Practical implications – The paper makes several recommendations for how businesses should evaluate, acquire, and use security technologies within their information security program. It also highlights business needs that the security industry is currently not fulfilling.

Originality/value – The ideas in this paper are entirely original. As far as the author is aware, there are no existing papers with similar ideas.

Keywords Data security, Asset valuation, Information strategy

Paper type Conceptual paper

Introduction

Seen from a distance, it might be easy to think that the field of information security is primarily about technology. Up close, it is clearly a multidisciplinary field that draws from economics, sociology, technology, business, and law.

Technology certainly plays a significant role in information security, but in this paper I describe why businesses should be cautious with their expectation of the value that security technologies can deliver.

Even though it might be counter-intuitive, there does not seem to be any empirical correlation between how much a business spends on information security technologies and a corresponding reduction in security incidents. CSO Magazine conducted a survey on this topic. Based on 7,596 responses from C-level executives in 54 countries, the survey determined that businesses that suffered security breaches did not spend any less on security technologies than businesses who did not suffer any security incidents. In fact, businesses that suffered no damages from security incidents in the year prior to the survey spent \$684 per capita less than the average for business that had suffered damages (CSO, 2003).

In the author's experience, businesses that have spent large sums on automated patch management products still experience broadly the same number of virus or worm infections as businesses that use comparatively primitive patching mechanisms such as scripting or deploying patches by hand. That observation is not meant to diminish the role of patching, as it clearly has many benefits, but the pragmatic



Information Management &
Computer Security
Vol. 13 No. 1, 2005
pp. 5-15

© Emerald Group Publishing Limited
0968-5227

DOI 10.1108/09685220510582629

viewpoint has to be that there are multiple factors that can influence the possibility of a security incident occurring. The amount of security technologies in use within an organization is merely one of those factors.

The problem is that businesses tend not be as balanced in their thinking. Spending on security technologies is widely viewed as a key metric within the security profession, as is spending on security as a percentage of overall IT budget. A suite of purchased security products is often viewed as “the security architecture” for the business.

The purpose of this paper is to analyze the value of security technologies overall, and to question if they should continue to be considered the central pillar within an information security program. As part of that analysis I make a prediction that the market for security technologies will soon become a commodity market. In a commodity market, the sole differentiating factor between competitors is price. Businesses will consequently come to view security technologies very differently, and security product vendors will have to make significant changes in their approach.

The commoditization of information technologies

Over the last several years the core building blocks of IT have become sufficiently cheap and ubiquitous such that practically every business can acquire them. There are very few businesses that cannot afford any computing capabilities, since personal computers have advanced to such an extent that their processing power, disk space, and networking capabilities now enable them to perform a huge number of business tasks “off the shelf”.

While it is true that larger companies have more challenging IT requirements, those challenges tend to arise primarily out of the scale of their environment (and from the complexity that comes with that scale), rather than from fundamentally new or different requirements. The solutions to those requirements are usually met, again, with off-the-shelf components, albeit in larger and more complex arrangements.

The core components within IT have thus become commoditized to a large extent. In a commodity market, the products offered by vendors are largely indistinguishable in terms of their ability to create value for the buyer – i.e. in the core functionality that they provide. Marketing efforts can shift consumer perception somewhat, but most IT professionals realize that there is very little significant difference between a personal computer made by Dell and one made by HP, for example.

In a commodity market, the primary basis for comparison between competing products is price. In the example of the personal computer market, Dell’s strategy has shifted that entire competitive landscape, because it is based primarily on driving down both costs and price. Many of Dell’s competitors have been squeezed out of the marketplace because they can’t compete with the efficiencies that Dell has created.

In the next Section I describe the factors that are driving the market for information security technologies towards a similar state of commoditization. I then discuss the implications of this change; the most significant of which is that businesses will focus their security efforts on how to achieve basic security capabilities for the lowest possible cost.

Drivers toward commoditization in the security market

There are three key aspects of the information security field that are driving the market for security technologies towards a state of commoditization.

The open nature of security technologies

Security products are sometimes referred to as “enabling” technologies. It is a claim that is usually made for marketing purposes, but it is a fundamental truth that technology has to be interoperable for it to succeed in the modern connected world. Experienced security practitioners realize that in almost all cases, the value of security derives from letting the right people in, rather than from trying to keep people out. You approach that goal by engineering the security of systems so that they can interoperate and work together.

When an online shopper makes a purchase on Amazon.com they rely on the secure sockets layer (SSL) protocol to encrypt the network traffic between their web browser and the Amazon.com web site. The benefit to the shopper is that SSL helps to prevent their credit card information (and their buying habits) from being revealed. The benefit to Amazon is that shopping online is made safer by using SSL, which is a critical requirement for their business model.

There would be no reason for Amazon to create a proprietary alternative to SSL, because the value of SSL derives from the open nature of the protocol. The benefit to using any protocol, by definition is that the protocol is known to all parties. Even if Amazon decided to create an alternative to SSL, they would have to open up the details of the implementation so that it could be incorporated into the many different types of web browser that a person might conceivably use to connect to Amazon.com to make an online purchase.

The value of a security technology usually lies in its ability to enable cooperation of some kind (think of connectivity as a type of cooperation). The more widespread and understood a cooperative technology becomes, the more value it can provide. A single FAX machine is useless, but the value of every FAX machine increases with the total number of FAX machines that exist, because the set of people you can communicate with grows. Similarly, a wireless security protocol is useless if it is not widely implemented, and so it is with authentication services, client/server security technologies such as SSH (secure shell), certificate services, public key encryption protocols, and the vast majority of other security technologies also.

Successful security technologies tend heavily towards having an open nature. (Of course, this does not necessarily mean that they are open source.) This open nature reduces the barrier for entry to those markets. Anyone can implement an SSH client, a public-key infrastructure based on X.509 certificates, or a RADIUS server, because these are all open standards.

Popularization of security capabilities

Security capabilities are attractive not only to businesses, but to individuals also. Individuals cannot usually afford to buy commercial security software that is targeted at businesses, and so this has led to a number of collaborative efforts to develop security technologies. Many people within the IT field, particularly hobbyists, are attracted to the study of security, and so there is substantial contribution to such projects. Two notable tools that have arisen from the open source security community

are the Snort intrusion detection system (www.snort.org) and the Nessus vulnerability assessment tool (www.nessus.org). Both are widely used, as are toolkits that enable the prototyping and development of security tools. One example is “Libnet” (Schiffman *et al.*, 2004), which is an API that allows the construction of customized network packets.

As a general observation, collaborative software is often used in much higher numbers than commercial alternatives. Consider the prevalence of the open source Apache web server, as described in Netcraft (2004), for example. Even if the functionality provided by open source security tools is assumed to be inferior to commercial products, individuals and businesses both find zero purchase cost very attractive, and so this drives widespread adoption.

Commercialization and the source of innovation

It is rare for businesses to develop security technologies in-house. Instead, they rely on a suite of products (technologies) bought from security vendors. The result is that the vast majority of technological innovation and new product development in the security field is being driven by vendors (the open source and academic communities are two exceptions; the third is very high-end companies like investment banks).

The result of this pervasive “buy rather than build” philosophy is that most businesses are employing almost identical sets of security technologies in almost identical ways. Because of this, if a business acquires a new security technology from a vendor, then there is no barrier that stops other competing businesses from acquiring the same functionality – either from the same vendor or another vendor whose product has similar features. The security market is overwhelmingly a capitalistic, commercial market in which security capabilities (products) are widely available for any business to purchase.

The open nature of security protocols, the popularization of security capabilities, and the extent of commercialization within the security industry all have serious implications for whether businesses can use security technologies to create competitive advantage.

Can security technologies create competitive advantage?

Businesses succeed or fail on the basis of competitive advantage or the lack of it. The three drivers toward commoditization described in the previous section point to the fact that security capabilities are becoming easier and easier for businesses to acquire. Indeed, as has been described, it is usually in the nature of security technologies to lean towards widespread availability.

If a certain resource is widely available, or if a certain capability can be easily duplicated, then it becomes very difficult for a business to create a competitive advantage using that resource or capability. The way that businesses come to view security technologies must inevitably become the same as the view of other commoditized areas within IT: once an acceptable level of functionality is reached, cheapest is best. This is very different to the current market for security technologies, in which the “latest and greatest” security products are pursued, seemingly as an end-goal.

There are other factors which are contributing to this shift, and these are described in the following sections.

Homogenization within the security market

Looking back at the history of security technologies, certain trends emerge, and those trends carry through to the present day. One clear trend relates to security technologies that enhance the capabilities of commercial operating systems. Historically it can be seen that if the functionality provided by an OS security product is deemed to be useful, then that functionality will eventually become incorporated into the OS itself. For example, vendors that used to sell directory services for the windows environment no longer exist (or they have reinvented themselves) because windows now has its native active directory.

This process of homogenization tends to be a gradual one, but it is inescapable because it is the result of market forces. Businesses do not want to buy security as an “add on”; they increasingly want security capabilities to exist by default.

Another noticeable trend is for large vendors to use their market penetration and existing sales channels to shape the underlying market. In the host-based protection space it can be seen that Cisco have priced their product very inexpensively in comparison to competing vendors. There is a widespread belief that Cisco actually takes a financial loss on the sales of this product. Why have they chosen to do this? The answer is because Cisco wants to own the mindshare in the end-to-end security infrastructure space. Having a widespread deployment of a certain technology within a business creates incentives for that business to employ additional technology from the same vendor (for interoperability, licensing, support, and many other reasons of efficiency). This is the concept of vendor “lock-in” in action.

Another example is in the workstation-based firewall space. The announcement by Microsoft that “Service Pack 2” for the windows XP operating system includes a firewall did not bode well for the vendors of personal firewall products, because it will eventually create a significant barrier for their entry to the corporate market (who are likely to already own windows XP). Understandably, businesses will not pay for functionality that is already built into their core platforms.

Given this trend, businesses may feel that the best strategy is to wait until emerging security capabilities become built into the products that they already own. Over time, the security capabilities of widely used technologies subsume third-party add-ons. In certain technology areas, it often pays to simply wait.

Feature-creep in security technologies

It is the nature of the IT industry to propel businesses onwards and upwards towards ever-increasing levels of processing power and functionality. But many IT professionals share a nagging feeling that the majority of employees within businesses could perform their jobs quite acceptably with a basic e-mail client, a basic web browser, and a basic word processing package on a PC with a fraction of the processing power that is considered “standard” today. An in-depth discussion of this issue is far beyond the scope of this paper (see Carr (2004) for a detailed exposition), but the general point is very applicable to thinking about security technologies.

The process whereby the performance of a technology product comes to exceed the needs of most of its users is termed “overshooting” by Christensen (1997). He describes why overshooting occurs very frequently in the computer industry. Manufacturers of IT products compete fiercely to advance the state-of-the-art, adding new capabilities to their products in the hope that they will become perceived as the market leader.

But this unrelenting drive for new features results in the functionality of the product overshooting the needs of the average consumer, who often responds by switching to a more basic, cheaper version from another vendor.

The rate of technological advancement within the security industry is ferocious, and so vendors are increasingly likely to become affected by the problem of overshooting.

As an example, Biancuzzi (2004) describes the most recent version of the “PF” firewall that is distributed as part of the OpenBSD operating system. The PF firewall contains functionality known as “stateful TCP normalization”. This functionality modulates the time stamps within network packets with a random number. The purpose is to stop an external party from counting the distinct number of time stamps within a stream of network traffic, and thus from inferring the number of hosts that sit behind a network partitioning device such as a firewall or router that provides network address translation (NAT).

Although this is an interesting feature, I suggest that it is a feature that is completely irrelevant to most companies. Purchasing decisions in the real world are not swayed by such technological minutia.

As an aside, an argument could be made that whenever a vendor adds additional functionality to their product, they increase the level of complexity. It is from complexity that bugs arise, and a security bug is simply a bug with a security implication. Simplicity is a prerequisite for reliability in most cases, and therefore, simplicity is a prerequisite for security also. A business would therefore, be truly advanced in its thinking if it requested vendors to remove unneeded functionality, rather than to add more features for competitive reasons.

Business priorities and diminishing returns

Before deciding to buy a new security technology, business should perform a pragmatic, honest examination of other areas that might provide more value. Many businesses do not have an IT test lab. A test lab is very important for testing software updates such as security patches, before they are applied to production systems. As mentioned earlier, information security concerns are often a subset of reliability requirements, and so if a business does not have the capability to test updates to production systems then that deficiency should be the priority, in preference to buying new security technologies.

The security press has a strong tendency to glamorize new and emerging aspects of the security field. Because of the weight of press attention it can be difficult for a business to objectively determine if it should invest in certain capabilities or not. Computer forensics is one example. The ability to forensically investigate a computer to attempt to determine what activity occurred on it (such as part of the investigation into a security incident) is useful only in proportion to the resources that are available to follow-up on those results. Most businesses who suffer a security incident rebuild the affected systems, patch them as best they can, restore the data, and then simply continue on, albeit probably more cautiously. They simply do not have the skills, funding, or motivation to re-architect their security or to attempt to trace the perpetrators. On television, “forensics” police shows get high ratings, but we can safely assume that most crimes are not solved with forensics, but rather with the use of simple processes that are usually not highly technological. We should view the role of security technologies with a similar pragmatism.

For many security technologies, the point at which diminishing returns sets in occurs at a very early stage. This problem, like many problems in security, has its roots in a fundamental disconnect between perception and reality regarding the level of risk. See Stewart (2004) for a discussion of topics around risk miscalculation and its implications for the information security field. It is sufficient to say here that businesses sometimes buy security products because they feel afraid, when in fact their level of risk is relatively low.

Business priorities and diminishing returns should be crucial decision elements when a business considers the adoption of a security technology.

Case study: intrusion detection systems

Businesses purchase security products because of the capabilities that those products claim to provide. In many cases, those capabilities have not matched expectations, and frustration and disappointment have been the result. Technology projects can fail for a multitude of reasons, but some observations can be made regarding root causes in the failure of security technology projects.

When evaluating a security technology, most businesses do not review the academic research within the field. It is often only in the research arena that the possible limitations associated with a particular technology can be found. Unsurprisingly, vendors of security products do not publicize research that points to intrinsic weaknesses within their products. Vendors, have marketing budgets, academics do not. The result is often a vast overestimation of the value that security technologies can deliver. To illustrate this point, I present the example of intrusion detection systems (IDS).

IDS is a technology that has grown immensely on the collective radar of businesses over the last five years or so. Tools such as IDS that give visibility into an environment are attractive, and the idea of “catching attacks as they happen” is an exciting idea. But many businesses have encountered significant unanticipated operational costs when deploying and operating this technology. IDS products have been found to be very high maintenance and require substantial expertise to operate in a truly effective, ongoing way.

The crucial point is that these operational costs are a result of the way that IDS products are designed. Unlike a firewall, there is an element of ambiguity in the way that IDS function. A firewall operates in an absolute way – it either passes a packet or not, based on its rule-set. An IDS has to attempt to infer whether an attack is happening. This guessing game leads to many instances where the IDS thinks that an attack occurred, when in fact it did not. Investigating these “false positives” drives up operational costs, as do false alarms where the user does not have sufficient understanding of their environment to distinguish between legitimate and illegitimate activity.

Companies who have struggled with their IDS implementations for these reasons might be surprised to hear that this issue has been known within the security field for over five years (at the very least). In a paper published in 1999 a researcher in Sweden noted that the value of an IDS hinges not on its ability to detect attacks, but rather on its ability to suppress false alarms, which drive up operational costs (Axelsson, 1999). Vendors of IDS products have viewed the false positive problem as essentially an engineering problem that might eventually be “solved”, but the truth is that the issue is

a result of the underlying methodologies that IDS vendors have chosen to employ within their products.

The operational costs of IDS deployments have given rise to the outsourced managed security services (MSS) market where businesses have attempted to offload the high operational costs of the technology onto an external third-party. The success of this approach can politely be described as “mixed”.

When businesses choose to outsource an aspect of their technology operation, they are stating that they do not wish to innovate within that area. There is no clearer indication that a technology has become a commodity than when it becomes a plug-and-play service.

Technologies or fundamentals?

For most companies there is probably more benefit to be realized in addressing the fundamentals of their environment, rather than with trying to keep up with the security industry’s latest trend. As a consultant I have talked with businesses that say they have no time to write documentation on their environment, and yet in the same conversation I have been asked to recommend what intrusion detection system they should buy. Which is ultimately more important to that company’s environment: having documented systems or deploying the latest security technology? Documentation might be boring to write, but leaving the environment undocumented is clearly a huge risk in terms of business continuity. The example given earlier regarding the widespread lack of foundational elements such as a test lab is also pertinent. These are foundational elements of IT that should not be usurped for the sake of fashion.

The roots of the security problems that many businesses face do not lie in a lack of security technologies, but rather in neglecting to address fundamentals and allowing the commercial security industry to dictate priorities.

New directions for the security industry

The way that the security industry has approached certain problems has shaped and framed the way that those problems are now considered. For example, vendors of intrusion detection systems compete with each other over whose product can detect the most “attacks”. This has had the effect of reducing a complex problem down to a numbers game that can be won by whichever vendor has the biggest marketing budget. The marketplace for intrusion detection systems has been locked into this mindset for years, and is only now emerging, even though the new methods that the IDS vendors have begun to implement have been known within academia for over a decade.

A similar situation exists with vulnerability assessment products. Vendors compete over whose product can detect the most “vulnerabilities”, but a common practice is for them to slant their internal taxonomy of vulnerabilities to make their figures look more impressive (Shostack, 2004). We should all acknowledge that such “creative articulation” is a disservice to the consumer because it creates a false perception of value.

The commercial security industry has attempted to bolster its sales using the above techniques because it is still struggling with how to “sell security”. At the present time, security products are sold on entirely amorphous criteria: either that the product is

needed in order to “be secure” (which presumes that that state actually exists), or because of “best practices” (i.e. fashion). Buying an intrusion detection system because everyone else bought one is not good strategy, and yet it is the prevailing purchasing strategy employed within businesses today.

In order to deliver real value, the commercial information security industry clearly needs to change how it approaches marketing and selling its products. Below, I present two initial ideas for how this can begin to be accomplished.

First, vendors have not yet chosen to understand businesses at a level that would allow security technologies to be integrated more closely with business processes. This would enable existing security technologies to be used far more effectively than at present. Straight through processing (STP), traffic and billing (T & B), and even payroll are all examples of business processes that it would be hugely valuable for businesses to be able to monitor, assess, and administer the security of in an end-to-end fashion. By focusing the delivery of their technologies in this way, security vendors would begin to make businesses view security not as a cost, but as a step that adds value to specific, existing business processes. The shift in mindset is from commodity to results, from product to solution. Another way to put this is that products (technologies) have to behave more like services.

Secondly, from the point of view of certain sectors, bigger security products (i.e. ones with more functionality) are not always better. Many businesses are not using security technologies such as firewalls or anti-virus systems because of concerns that they could impact very demanding CPU or network latency requirements. In those situations, a stripped down, minimalist security product that provides a base level of security with a footprint of a provable size would be seen as highly attractive. Nothing like this is available today.

Where are we on the S-curve of market penetration for security technologies? The security industry would emphatically say that we are on the up slope. That may possibly be true, but if the current direction is not changed, the top of the curve will arrive a lot sooner than the security industry expects.

Conclusions

The topics discussed in this paper have implications both for businesses and for the information security industry itself.

For businesses

It is crucial for businesses to be able to distinguish between resources that have the ability to create competitive advantage and resources which are, or are becoming, a commodity input. Information security technologies are becoming a commodity input that should not be expected to create a competitive distinction.

If security technologies cannot provide competitive advantage, should they be perceived simply as a necessity? After all, no business wants to be insecure. That is true, but in necessity markets in which a base level of functionality is all that is desired, the sole differentiating factor, between products, becomes price. Businesses will become increasingly reticent to pay for complex security functionality where a base level will satisfy them. The market has already demonstrated that it will not pay for high-end security where other competitive differentiators such as scalability or ease of use are deemed to be more important. The OpenBSD operating system is considered by

many information security practitioners to be the most “secure” operating system available, and yet its use in the business world is close to non-existent. The requirements that businesses place on security technologies will become no different to the requirements placed on any other IT product: cheap to buy, cheap to maintain, and cheap to upgrade (i.e. simpler).

There is little advantage in being an early adopter of security technologies, unless you are uniquely positioned to be able to leverage the temporary advantage that the technology might give you. Even if you can do that, you would expect your competitors to be able to copy you relatively easily, given the tendency for security technologies to become commodities sooner rather than later. A cautious approach is best; one that takes advantage of the inevitable popularization, commoditization, and price-reduction of the technology. Follow, don't lead.

Addressing business fundamentals should always take priority over the purchase of new security technologies. Test labs, documentation, business continuity and disaster recovery plans are all examples of foundational elements that contribute overwhelmingly to security.

When considering adopting a new security technology, a business should determine if its existing infrastructure can already provide similar capabilities. Most companies already have most of the basic security capabilities that they need, due to the native security functionality that is built into the products that make up their infrastructure. The trend will continue for major vendors (such as operating system vendors like Microsoft) to implement increasing amounts of security functionality within their products.

The results of academic research are often the only place where a true picture of the risks associated with security technologies can be found. Businesses should consult research papers published in journals and conference proceedings, and assiduously avoid “research” published in populist security magazines.

The Pareto Principle, also known as the 80-20 rule, suggests that performance depends disproportionately on doing a few things really well. The use of technologies might not be one of those pivotal factors. The focus of an information security effort within a business should be on pursuing activities that provide the maximum return. Information security problems tend to manifest as technology problems, but they have their roots in organizational and process deficiencies. The best return on your investment will probably lie in areas other than technology.

For the commercial information security industry

The marketplace for security technologies will become, and in some areas has already become, a commodity market in which the capabilities of the products that populate the market can be easily acquired by all businesses. Because of this, consumers will increasingly focus on acquiring basic levels of acceptable security for the lowest possible price. Commodity markets are cutthroat, and so ruthlessly driving down price and creating efficiencies to reduce internal costs will be the only way for security vendors to survive. As an example of the impact of such a market shift, it can be seen that commoditization has transformed the managed security monitoring (MSM) market into one with tiny margins and huge turnover in customers.

The race by vendors to implement increasing amounts of functionality within security products may actually be detrimental to the security of their customers.

Security derives from simplicity in most cases, and so it becomes increasingly difficult to verify the security of products that are heavy with the weight of excess functionality. If the general marketplace comes to realize and acknowledge this fact (which is not necessarily a given), then vendors can expect consumers to look for smaller, more lightweight security products that function in very specific roles and that emphasize correctness over marketing-driven features.

Businesses will begin to employ extensive criteria that allow them to examine the costs associated with security technology projects, and to make go/no-go decisions on the basis of that data. Vendors should anticipate increasing levels of scrutiny, and work on empirical means to convey evidence of value (assuming that it exists).

From a pessimistic point of view, if margins are falling because of commoditization, features are increasingly devalued in consumer's eyes, and vendors can expect that buyers will begin to impose stricter and stricter criteria on purchases, then vendors may wish to consider if they even wish to stay in the information security technology market. There is increasing crossover between security and other areas of IT (such as network management, availability and redundancy monitoring, and so on), and so "escape routes" do exist.

The market for information security technologies is almost certainly over valued. There is a substantial amount of econometric research that remains to be done in this area.

References

- Axelsson, S. (1999), "The base-rate fallacy and its implications for the difficulty of intrusion detection", *Proceedings of the 6th ACM Conference on Computer and Communications Security*.
- Biancuzzi, F. (2004), "OpenBSD PF developer interview", available at: <http://onlamp.com/>
- Carr, N.G. (2004), *Does IT Matter?*, Harvard Business School Press, Boston, MA.
- Christensen, C.M. (1997), *The Innovator's Dilemma*, Harvard Business School Press, Boston, MA.
- CSO (2003), "The state of information security 2003", *CSO Magazine*, October.
- Netcraft (2004), "Netcraft web server archives", available at: <http://news.netcraft.com/>
- Schiffman, M. *et al.* (2004), "Libnet", available at: <http://packetfactory.net/projects/libnet/>
- Shostack, A. (2004), Personal communication.
- Stewart, A. (2004), "On risk: perception and direction", *Computers and Security*, Vol. 23 No. 5.