Easy does it

The paradox of information security is that while the best products have necessarily complex functions, they must also be easy to use, writes Rob Buckley

Information security is a complicated discipline. It requires a deep understanding of people, processes and technology to prevent an organisation's systems and data from being compromised, either accidentally or deliberately. So, to some, 'ease of use' in security software is a misnomer – infosec should be hard, shouldn't it?

Yet the innate complications of infosec can have negative effects: employees might stop bringing their own devices to work if the kit is made significantly harder to use as a result of security; fed up with attempts to block or restrict their access, they might add cheap WiFi routers to networks; unable to remember many complex passwords, they are likely to duplicate these across multiple, weakly protected websites; and being harassed by endless security pop-ups could well encourage them to unthinkingly click on fake ones.

The problem is not restricted to end-users. Gartner analyst Greg Young says up to 98 per cent of firewall breaches are caused by misconfiguration. Meanwhile, SIEM logs go unread or are switched off because of false positives and the time required to deal with them. Systems are not integrated because they are just too hard to combine. Even jobs are left unfilled because the necessary expertise is either unavailable or too expensive.

So, is there a happy medium between the desire for simplicity and the need to be secure? And how much attention are vendors and CSOs paying to the issue?

Easy living

Every vendor, if asked, would claim that ease of use is important.

"It's of great interest to us," says Ville Hämäläinen, director of R&D at Stonesoft. "We claim to be the most usable in the industry."

Jody Brazil, president and CTO at FireMon, says: "We sweat bullets day in, day out to make sure our software is easy to use."

Andy Jacques, general manager for EMEA at Good Technology, adds: "It's absolutely the core of the Good for Enterprise product."

Of course, no software vendor is going to state that its software has deliberately been made as difficult to manage as possible, or that the concept of usability is not something they bother with. However, clearly some products are harder to use than others.

Morten Stengaard, director of product management and quality assurance at Secunia, has a background in consumer software, which he says is much more user-friendly. "Security vendors have failed in the past to make things easy to use. They have focused on features, not the total cost of ownership and how much work there is for the user," he says.

Garry Sidaway, global director of security strategy at Integralis, agrees. "Few vendors ask us how we implement [their software] and reduce complexity for our clients. We try to talk to them about their issues, but I don't see it changing," he says.

Good Technology's Jacques insists that his company's software is easy to use. "It has an intuitive look and feel, and more than one million users. People find it instantly familiar," he states. Productivity is an important requirement, he adds, claiming that the too 'heavy' security of rival software restricts workers.

Jacques cannot specify how many Good Technology staff work on ease of use, but says third-party companies carry out user testing, while the good.com forum is another source of feedback and advice. His metric for determining the product's ease of use? "We have more than one million users," he repeats.

Nevertheless, Chris Hewertson, CIO of IT services provider Colt, reports that when he implemented Good Technology's mobile device management software to secure iOS devices and their data, his users rebelled. "They didn't like it because it didn't feel like an Apple app," he says. In other words, the software lacked the ergonomic design that users have come to expect of their consumer products – so Hewertson chose a different solution.

It goes without saying that usability is in the eye of the beholder, and people are notoriously fickle when it comes to technology. It should be no surprise then that vendors put in varying amounts of effort into usability – after all, you cannot please all of the people all of the time.

Steven Hope, technical director at Winfrasoft, says his company makes no formal studies of usability, but "internally, a lot of people are dealing with customers and know what a lot of the common complaints are". New versions are tested among customers as soon as possible, Hope adds, but "we don't do any particular focus groups".

By contrast, Stonesoft's Hämäläinen claims that a third of the company's developers are dedicated to the product's interface and its ease of use. These developers, he says, try to use "known concepts" to make the user interface familiar, admitting: "We've taken many examples from Apple, iTunes, web

browsers and social media sites." Stonesoft puts its product through regular testing, not just with existing customers, but also among students with no experience of security software.

Familiarity and expertise

Familiarity is important, since it speeds up the process of finding one's way around new software.

Sian John, security strategist at Symantec, says: "For Symantec, ease of use is a very big focus, although we've not always been as successful as we could have been." She adds that whenever the company acquires a new product, it looks at the interface to see not only if it can be improved and made easier to use, but if it can be made to look like Symantec's other products.

The irony here is that in making these changes, the company risks alienating existing users who are already familiar with the products. John says: "You'll get tech security people who'll say, 'Oh, you've taken things away.' People have spent ages learning this software and to them it's second nature. They'll get focused on a widget, even if it makes the console more confusing."

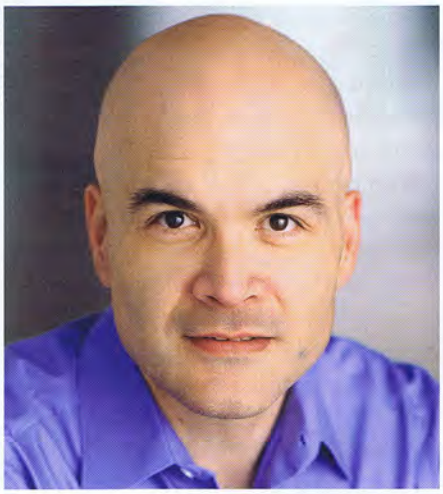
Then there is the problem of 'feature creep'. Secunia's Stengaard says that when he arrived at the company, it was so focused on what new features it could add with every release that it had neglected ease of use in its AV product. "We were feature-focused with lots of graphs. Yet something like finding the scan button proved difficult," he explains. In the next version of the software, Stengaard started with a near blank slate for the interface that included only the important features and would automate processes as much as possible. He brought in a new design team to work on the interface, led by someone with experience of both consumer and security software.

However, Stonesoft's Hämäläinen argues that even with the best will in the world, "the domain is so difficult – we do deep-packet inspection, VPN, anti-spam… if you want to set up a VPN, you have to know about cryptography and protocols, so we can't make it too simple". All the same, Stonesoft continues to try to reduce the complexity of processes, to make products easy to set up and to ensure that they contain a good set of defaults – so removing the headache for most users.

Overcoming complexity, particularly in a heterogenous environment where there might be devices from various vendors, is an area where FireMon has carved a niche for itself, offering a management console for multiple firewalls. "We focus on configuration management," says Brazil. "More often than not, configurations are incorrect, with 40 per cent of firewalls completely useless. Two-thirds of configured firewall policy has no business purpose. And that's purely down to complexity."

With perhaps several hundred firewalls, each with between 300 and 500 rules, the path to misconfiguration is well-trodden. While interface improvements, such as Check Point's graphical editor, have helped with the management of individual firewalls, dealing with them en masse has become a serious ease-of-use problem that the vendors are not focused on addressing, Brazil says.

What's more, there is now more than one kind of professional accessing security technology, something that


Steven Nereyko

vendors are only slowly waking up to. "In the past, security products used to be sold to security experts, and it was that combination that was then sold to the non-expert," says Tim Keanini, chief research officer at nCircle. "As security permeates throughout an organisation, you're asking, 'To whom is this usable?' The same tool that is absolutely usable to the security professional is completely unusable to the auditor."

Thus nCircle has created different interfaces for different types of users. "Over the past five years, we have restructured the product so it's completely different for different personas, because you don't want to make it easy to use for someone at the expense of others," says Keanini.

Usability vs efficacy

To a certain extent, vendors have perhaps failed to prioritise the interface because doing so goes against the way security technology is procured, argues Dave Taylor, vice president of corporate strategy at WatchGuard. "If Cisco has sold to company A, and all I can say is that my product is 250 times easier to use, there's a challenge to get funding. I have to push the security efficacy," he explains.

Equally, it is hard for a CSO to pitch a new product to the board when the only thing that differentiates it from existing technology is that it is easier to use and less likely to lead to misconfiguration.

> **As security permeates throughout an organisation, you're asking, 'To whom is this usable?'"**
>
> Tim Keanini/nCircle

Furthermore, adds FireMon's Brazil: "Customers expect good management tools, but they're not willing to pay much more for the tools than for the underlying technology."

Despite all this, ease of use is likely to become of greater importance in the near future. "Ease of use in management will continue to emerge as a key differentiator in the industry," predicts WatchGuard's Taylor. "It's going to become a battleground with TCO-type analyses."

He points to the early days of AV when vendors fought over product features and the number of virus definitions, with usability and performance largely forgotten about. "It was an arms race. But what happened was that machines became so unusable with AV that users would hit Ctrl Break to stop scans, creating a security risk. McAfee realised the problem, stepped back and stopped the arms race," Taylor says.

With budgets being cut, skilled staff at a premium and complexity ever-increasing, the day could be nigh when usability is as important a consideration as a product's features. ■

CASE STUDY: LNT GROUP

When LNT Group wanted to roll out 1,700 iPhones to staff, Leigh Ellis, head of web and marketing, knew ease of use was going to be important, not just for security but also for deployment. The group has six core businesses in sectors including construction and chemicals, but Ellis says the main concern was its nursing home staff who had "not much IT knowledge". Training was not an option, so something intuitive was paramount.

In particular, Ellis was looking to use a mobile device management (MDM) platform to maintain the iPhones securely and simply. He conducted a questionnaire to see whether the staff had used smartphones before and to what purpose. "Most knew someone who had a smartphone, but they had only used phones for the basics themselves," he says.

After selecting a few MDM products with the desired features, Ellis conducted trials among staff to see which they were able to use easily. "The same groups of people found the same products harder or easier to use, so it was simple for us to see which one we wanted," he says. LNT ended up choosing Absolute's MDM software, mainly because of its ease of use.

"Normally, when you're finding files and attachments, there can be multiple copies," says Ellis. "With Absolute Safe, there's one repository for all files – you don't have to scroll through emails." An app store within the interface also allows users to download and update approved apps, including ones authored by LNT, in a manner identical to the Apple App Store.

The system also simplifies administration. Ellis has to administer most of the security systems in use at LNT himself, since few others have the necessary technical training. However, the interface of the Absolute software is so simple that non-technical users can configure the MDM without prior training, saving Ellis some of the burden.

"It takes just five minutes to set up. Some of the systems require you to use RegEx commands just to specify who can access which systems at which times. Here, you just tick the boxes," he says.