encription
IT Security Services
www.encription.co.uk
01905 754440

THE 10 DARKEST TRUTHS ABOUT INFORMATION SECURITY

Securing information should be top of the IT agenda for companies of all shapes and sizes. It is also one of the most misunderstood disciplines within IT. A good day for a security professional is when nothing bad happens, when no one really knows they are even there. Most security people are never going to be the hero, but they don't want to be the villain either.

Unfortunately, the most proficient security professionals have a hard time getting and maintaining visibility with senior management, who tend to get lulled into a false sense of security when nothing bad happens. The fact is, complacency will get you killed. New attacks are happening at a ferocious pace, users are willingly giving away their private information, and today's standard defences are no longer enough to protect critical information. Those that cannot make a compelling case for continued investment in proactive defences against these attacks have no chance against the bad guys.

A pragmatic way to show the importance of security is to tell senior management about the 10 "darkest truths" of information security. Many of these points are hard to accept, and most of the industry will not acknowledge them because it makes it abundantly clear that today's defences are not getting it done.

Truth No. 1: *You will be hacked.*
The sad truth is that your network and applications can be compromised at any time. There are talented and determined hackers who can make mincemeat out of your firewalls and other protective devices. It usually takes them less than 10 minutes, and there isn't much you can do to stop it. So the first step is to acknowledge there is no such thing as 100% security. That doesn't mean you shouldn't try. Most of the people out there are neither talented nor determined, which means that a strong, proactive defence can keep those people at bay.

Truth No. 2: *You can't get everything done.*
Running a vulnerability scan against your current network will be very instructive. You'll find out that Truth No. 1 is absolutely true. In fact, most penetration tests will get into the network. You are vulnerable, and the list of things to fix can be very long. You won't be able to get everything done.

That's right, you can't get it all done — so don't even try. Spend more time figuring out the most important things to do. What issues present the most risk to your environment, to the systems that keep your business running? Get that done and then move on to the next task, It ensures you make the most of every day.

Truth No. 3: *Users are the path of least resistance.*
Hackers are concerned with only one thing: getting into your network. It doesn't need to be fancy, and it doesn't need to be clever. The attacks just need to work. Nowadays, the easiest way into your network is through your users. Users click on things in their email. They fall for phishing attacks. They surf to bad sites. Even worse, most of these issues could be avoided just by telling your users what not to do. Spend a few hours teaching them what to avoid, how to detect an attack, and when they should call for help. It will be time well spent.

Truth No. 4: ***Applications are the lowest hanging fruit.***
Firewalls have been in use for the better part of the last 10 years. They work pretty well and — bolstered by intrusion prevention and other perimeter defence tactics — your network is relatively hard to penetrate. It's not impossible, but it is relatively hard, especially compared to web sites. Web applications, on the other hand, are porous. (Think Swiss cheese and you'll be close.) Whether it's an SQL injection attack or cross-site scripting, your applications are a mess — literally.

Somewhere in the order of 70% of web applications can be compromised via very simplistic attacks. We are severely resource constrained, needing about 10 times as many web application testers just to test 2% of the applications out there. If there is a positive spin here, it's that there aren't enough bad guys to go around either, so the hope is that you won't be targeted. But hope is not a strategy. Do a web application scan and patch up the holes ASAP — before your number comes up.

Truth No. 5: ***AV is not enough.***
Mobile devices are one of the most vulnerable aspects of your environment. Employees connect to your network over wireless hot-spots and in coffee shops, both of which carry the risk of being compromised. These endpoints typically are sent out into the cold, dark world with nothing more than a standard antivirus defence. It's not enough. You want to add more sophisticated defences, including antispyware, host intrusion prevention, application control, and data encryption to protect those devices. The good news is, many of these functions are increasingly being bundled into a single offering that can be managed centrally. That's a good thing.

Truth No. 6: ***You don't need to do everything yourself.***
Another commonly held misconception is that you need to do everything. Resources are a critical constraint, especially for midsized businesses, so get help. There is no award for struggling to get everything done and then missing something important. A majority (upwards of 60%) of successful hacks occur as a result of simple configuration errors, not a lack of defences.

There are some functions, such as email security or firewall monitoring, that can be done more effectively by someone else. By outsourcing some of these "less than" strategic functions, you can spend your time on tasks that will make more of a difference. This will allow you to prioritise and get through the list that much faster.

Truth No. 7: ***Getting hacked isn't the issue — the issue is how you deal with it.***
Ah, the best-laid plans — but the reality is, you will still end up with some kind of incident.

In the annual FBI/CSI study, about 60% of companies say they had a problem in the last year; the other 40% don't know they did. At some point, your number will come up. The difference between success and failure is how you deal with it. So build an incident response plan and do it now.

Make sure you know exactly who is supposed to do what at the moment of truth. Ensure that senior management is on board with your plan and that you will be able to recover and remain operational.

Truth No. 8: *PCI DSS is not a joke.*
Compliance has been the paper tiger of security for years. Everyone talks about it, and vendors try to sell you on it, but the powers that be have chosen not to enforce it. So to date, there have been no adverse ramifications to not being compliant — until now, that is.

PCI (the Payment Card Industry Data Security Standard) seems to be the first of the regulations with "teeth." For example, CardSystems lost its ability to process charges, due to a data breach. TJX/TKMAXX is being hit with class action suits daily. The pain and the threat is real. This could be only because the credit card companies and banks have not figured out a way to place the blame and financial impact of data breaches on the retailers. Any organisation that handles credit cards, no matter how few, is subject to the regulation, so take it seriously. Don't end up on the front page of the newspaper.

Truth No. 9: *The auditor is your friend.*
Most security professionals have a kind of "hate-hate relationship" with auditors. They figure the auditor will call them idiots and show how incompetent they are. It couldn't be further from the truth. Auditors are actually after the same thing as you are, protecting the information and business systems of your company.

If you treat the auditors as allies and work *with*, not *against*, them it changes everything. Come clean with the auditors. Tell them what they need to know.

Truth No. 10: *There is no silver bullet.*
A lot of security professionals want to write a cheque and make the problem go away. Unfortunately, if it were that easy, everyone would be doing it. Security is a process, not a product. It's a culture, not a service. Only through consistently evaluating the risks of every interaction with applications and data can sustainable security be achieved.

The hard work begins by understanding which of your business systems are most critical to your operations. Then you incrementally secure each exposure, and — over time — you can get to the point of security nirvana. But to be clear, it is neither easy nor quick, but it's important. You have no more valuable assets than your customer data and your intellectual property. Protect them wisely.

Summary
Many of these "truths" are counter-intuitive. They are meant to paint an honest picture, not to create a hopeless situation. You can secure your environment, and you can do your job. You need to be smart about it, but accepting the common wisdom of what security should be is not the way to do it.

Think differently and act differently — and you'll find security success.