Systems (DCS). It is also referred to in some publications as HMI (Human Machine Interface).

Since SCADA is used as a control mechanism for chemical plants, electricity generation, electric power transmission, electricity distribution, district heating and other CI elements, SCADA systems themselves need to be protected against cyber attacks. The US 2002 Document on "21 steps to improve Cyber Security of Scada Networks" states:

"SCADA networks [are] potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruption to the nation's CI." "Single points of failure must be avoided and cyber security defense must be layered to limit and contain the impact of any security incidents."

The document is divided into rules giving clear guidelines as to what to address:

- Rule 16: identify cybersecurity requirements and Rule 20: roles & responsibilities of all individuals.
- Rule 19: establish back-up and disaster recovery plans.
- Rule 21: deals with "social engineering" threats and user training requirements.

Evidently, normal best practice security rules apply to the protection of SCADA networks including self-assessment, defence-in-depth, ongoing risk assessment, regular penetration testing, system hardening, minimizing external remote connections and so on.

Security awareness programmes and campaigns are also key to the success of countermeasures against cyberterrorism.

Notwithstanding the role of the governments who through CERT initiatives as well as other key legislation and standards promote good governance (e.g. Sarbanes Oxley, European Data Protection Directive, Payment Card Industry Standard), there is a definite requirement for improved, more in-depth public-private cooperation to address the threat of terrorism through cyberspace. It is, however, early days and so far no human death has been clearly linked to cyber attacks whether they were terrorism or criminal acts. Nonetheless, this is an item which has become high on the agenda of many industry analysts and it is very likely the industry itself, along with the government initiatives, will continue to put pressure on businesses as well as citizens to take basic security steps to help fight cyberterrorism and protect our critical infrastructure.

About the author

Mathieu Gorge is the Managing Director of Vigitrust – an Ireland-based security consultancy.

Profiles in cyber courage #1: Fred Cohen

Richard Power and Dario Forte

Richard Power | Dario Forte

Dario Forte and Richard Power have identified a number of security gurus who have made a difference in the IT security field. Every second month our authors will interview an established expert. The first profile focuses on Fred Cohen, a pioneer who first described a computer virus.

In the early 1950s, while recovering from back surgery, Sen. John F. Kennedy of Massachusetts (who would later become the 35th president of the US), wrote a book entitled *Profiles in Courage*. It became a bestseller and helped propel him to prominence on the national scene. *Profiles in Courage* highlighted the bravery and integrity of eight Senators, throughout US history, who defied political pressure and public opinion to do what was right.

This year, every second month, the *War & Peace in Cyberspace* column will feature a new series – *Profiles in cyber courage*. In this ongoing series, we will focus on colleagues who have made significant contributions to the field of cybersecurity, and conduct in-depth interviews on timely and vital issues.

Our first profile in cyber courage highlights Fred Cohen (http://all.net), who has been operating beyond the frontlines of cybersecurity for more than 25 years.

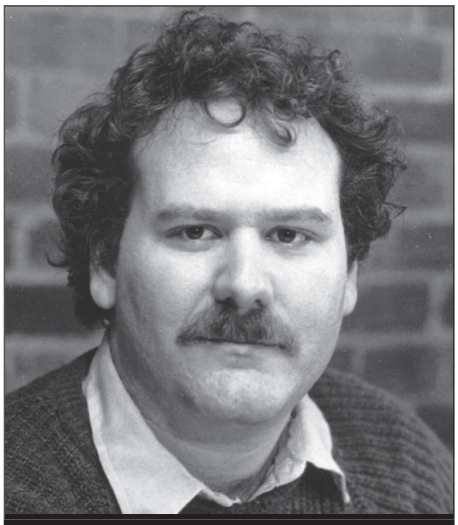
Dr Cohen is a world-class researcher, educator and consultant. He is also a prodigious author. His "Chief Information Security Officer's (CISO) Toolkit" is a collection of tools that CISOs can use to overcome the real-world challenges that confront them. His *Fraud, Spies and Lies, and How to Defeat Them* is an exhaustive exploration of techniques utilised by fraudsters and intelligence operatives. It shows how to conduct investigations and counterintelligence operations to protect yourself and your organizations.

Forte & Power:

We all have CVs, and book jacket biography blurbs, but instead we would like to hear your thoughts along the following lines: How many years have you been working in cybersecurity? What do you think has been most rewarding about it? What do you think has been most disturbing or discouraging about it? What surprises you – if anything – about where the field is today versus where it was when you began your career?

Cohen: early start

I started in information protection in the 1960s when I was a school child. At that time very few children used computers, but I programmed when I was in grade school. I knew a lot of other kids who were in Project Solo at the University of Pittsburgh and used to spend time with them. I spent time using and doing administration on computers at the university, and programmed computers for my father's Nuclear Physics Lab at the university. Some might be surprised to know that input overruns, protection faults, timing faults, and many of the other issues we encounter today were around then, but these same things were happening at that time and the folks I knew were on the bleeding edge of them. Some were breaking into systems – mostly local systems – to gain authorized access when authorization mechanisms were inadequate and they had to get things done. I didn't break in, but I watched and learned. Then at high school I became systems administrator for the high school computers because I read the manuals and understood more than anyone else about it at the school. In college I worked as a computer operator in the early days of the ARPAnet and had to help clean up the messes left by others. I collaborated with a fellow student to build a digital and analog timed permutation lock, and then started to work on US Department of Defense (DoD) projects securing AutoDIN and AutoVON – early DoD networks – and designing secure protocols for the next generation of these networks. The most rewarding part to me is frustrating bad folks, teaching, and learning about new things as a researcher. The most disturbing thing is that we keep putting more risks on weaker and weaker systems and depending on more and more people we do not know and cannot reasonably trust for things of greater and greater importance. Nothing is really all that new under the sun in computer security. Maybe every five years I read about an interesting research area and enjoy it. Other than that, I am mostly interested in my own research, which is moving more and more towards governance and human issues, which seem to dominate the field as they always have.



Dr Fred Cohen

> "People won't improve by using a different OS"

On legend

Power & Forte: Are you the father?

Just to get it out of the way – give us the definitive answer as to whether or not you were really "the father of the computer virus"? How did this legend start?

Cohen:

I was the person who first came up with the name, published all of the first scientific articles and turned it into a real field of scientific study. But the first program that reproduced was – I believe – done in the 1950s by Moore – a very well known theoretician and practical man who implemented a hardware configuration that reproduced.

On Microsoft

Power & Forte:

We think Microsoft is part of a large security problem rather than part of the solution. Is there any viable alternative to the Microsoft operating environment; and if so, for what types of businesses or organizations? What are the alternatives and how do they measure up on security issues? If not, can we expect any feasible options in the foreseeable future?

Cohen: Anti-competitive

The reason that Microsoft has had and continues to have inadequate protection for the environments it operates in is that those who buy their products continue to do so. Apple has a fine operating environment – based on Unix, as do many other products – including Linux-based products. But the lack of government response to anti-competitive practices combined with generally conservative views from CIOs and others has limited competition effectively. I don't think Microsoft is "at fault" or "to blame." People prefer McDonalds to most other restaurants, not because it is the best quality food – but because it is adequate to their perceived needs at the best price for that criterion. Lots of businesses use OSX and Linux today, of all sorts, and the percentages are growing. But the major security issues we face are not strictly from the external operating system weaknesses, and to think that fixing these would have a significant long-term impact would be foolish. People issues dominate and people won't improve by using a different OS.

On training

Power & Forte:

Could you give us your perspective on the current quality and efficacy of technical training in cybersecurity? Are there any real

Cohen's top US recommended universities for IT security:

Technical courses:

- Naval Postgraduate School, Monterey, California.
- UC Davis University of California.

Forensics:

- The University of New Haven, Connecticut

Technical management of infosecurity:

- George Mason University, Washington DC

programmes (academic, government or other) available to produce well-prepared and well-trained people? And if so, could you name some you consider worthy? What are the major failings in the training of cybersecurity professionals? How could it be done better? And, of course, what is your view on professional certifications? What is your view of the relative strengths and weaknesses of certifications? How could it be done better?

Cohen: Academia is on the up

Academics are getting far better – for example, a dozen or so schools actually teach reasonable curricula these days and more are popping up. The SANS and CSI types of groups fill a niche for professionals wishing to stay aware and learn more, but they are hardly at the level of what a decent university course covers. The best schools in my view are UC Davis and Naval Postgraduate School for the technical side, the University of New Haven for the forensics and law enforcement side, and George Mason for technical management of information security. But others do a reasonable job. Training is certainly a good thing for people that have immediate needs to do specific technical tasks, but education is intended to last a lifetime, and that makes a world of difference. The in-depth theoretical knowledge I gained was and still is invaluable, while training courses just don't give that sort of knowledge in my view. The current certifications are good in that they show a level of knowledge. It's not a very high level of knowledge, but it is worthy of attention that someone has studied enough to get that far, and all the more so in a field full of charlatans and snake oil salesmen. We need to change this by getting universities more fully engaged in the educational process and promoting those with advanced scientific knowledge. We need to really support leading edge research, which we do relatively little of, and we need to support bleeding edge ideas instead of the same old stuff all the time. But the government is stodgy when it comes to research and the people who are already funded are most commonly the judges of new people getting funding, so the inbreeding is problematic. Private funding is pathetic and always tries to profit in a year or two, and this does less to advance the field than its promotion of the funding companies.

> **"We need to support bleeding edge ideas instead of the same old stuff all the time"**

On awareness & education

Forte & Power:

Awareness and education, if developed wisely and delivered properly is economical and effective. And yet, it is so terribly under-funded, misunderstood and under-utilized in most organizations and societies. Why? Phishing is, arguably, an excellent example of a multi-billion dollar problem that would be significantly reduced through aggressive awareness and education programmes for the workforce and the public. What are your thoughts on the failure, on the part of corporations and governments alike, to invest in really powerful awareness and education programmes? What do you think should be done in this area?

Cohen: awareness is cheap

Education and awareness are the opposite sides of the knowledge spectrum with training in the middle. The awareness issue is really key regarding phishing and, in many cases, viruses. Awareness goes well beyond these issues, of course. In almost every assessment we do, we find that it is a simple matter to walk into a facility, plug in a small wireless access point, hook it up to the network, and gain unfettered access to the network. With a few technical manoeuvres after that we gain access to lots of information. A safe work environment depends on physical control over the space, and yet people don't even react to strangers in the workplace in most cases. Based on these experiences, I wrote a 50-page booklet for awareness that, if followed, would eliminate almost all of the security-related issues associated with users in most enterprises. Of course it has to be reasserted every six months or so because that is how long such awareness typically lasts. And that is another fact many people don't seem to grasp. Awareness is inexpensive (in the order of US$10 per year per user), highly effective (eliminates around 90% of the things that go wrong), and poorly done. It's inexpensive, easy to fix and can be done in short order – easily in a period of a few weeks. But this sort of programme is not in control of the technical department and involves no technology (although you can use technology if you wish). Therefore, it has no advocates to lead its implementation within most enterprises. Finally, it is important to understand awareness done well tells you what to notice and how to react to it. In other words: when you see this, then do that. In many cases, it isn't done this way and ends up less effective.

On forensics

Power & Forte:

Forensics is one of the "hottest" areas of cybersecurity. Could you tell us where you think it is headed? How far has it come? What are the biggest problems? What are people missing about this topic? Is it possible to confuse a jury like what happened in the infamous OJ Simpson case in the US? The OJ Simpson defense team employed a DNA specialist lawyer to tear apart the prosecution's evidence and befuddle the jury. Generally, could forensic evidence in a cybercrime case withstand even a cursory

challenge in a court room, provided the defendant had the money to contest it?

Cohen:

Forensics is a particularly interesting area for me because I teach it to graduate students and work with many of the top experts in this arena. I think it is heading toward true professionalism, a direction that the rest of information protection is lagging in sorely. When I testify, my PhD and years of experience are a big help in lending authority to my words. Of course I have to be careful in what I say and use a strong scientific basis for my results. I do digital crime scene reconstructions, which are quite expensive in many cases, but get real answers. A lot of expert witnesses who assert that this is how something works find out that reality is not how they see it when faced with a real expert on the other side. As the legal community starts to realise this, it will draw out the high priced real experts and start to punish the snake oil salesmen in the extreme. And I view this as positive – just what we need to start forcing reasonable and prudent approaches, worked out solutions rather than guesses and assumptions, and serious research rather than pundits and positioning. In answer to the second part of your question, much of today's cursory evidence falls by the wayside when examined by experts. I have personally been involved in three cases where seemingly strong evidence was completely unraveled by a solid examination of the facts and careful reconstruction of the circumstances. In two cases innocent people were kept from wrongful convictions. Money is certainly an issue, but more important in my mind, is the location of real experts wiling to do the real work and lawyers who are willing to let them seek the truth regardless of how the chips may fall.

On knowing what's what

Power & Forte:

In 2007, what are the most important questions any cybersecurity professional should be able to answer about their organization's security posture? And what answers should their executives expect from them?

Cohen: Five questions & answers

- Question number one should be: "How does the business work and what are the business impacts of protection failures of different sorts in different places?"

  The answer should be: "We have a business model and here it is. The most important consequences are listed from the worst down to the acceptable loss threshold."

- Question number two should be: "What are the thresholds for consequences that we use to determine protective levels?"

  The answer should be – "The CEO specified the following levels..."

- Question number three should be: "What are the duties to protect as defined within our enterprise?"

  The answer should be: "Here is the list of duties as agreed to by top management and the business units and per the requirements of COSO."

- Question number four should be: "How much is protection costing us, and how much are incidents costing us – to a first approximation?"

  The answer should be: "Protection costs are about X and losses are running in the order of Y. The costs of X are about 2/3 of the total program costs while losses account for the other third." (This is about optimal).

- Question number five should be: "Do you have the necessary power, influence, feedback, and resources to get your job done?"

  The answer should be: "Yes I do."

Of course, the reality is that these are almost never the answers given because programmes are almost never operating so effectively. These are among the most important things that need to change.

About the authors

Richard Power (www.wordsofpower.net) is an internationally recognized authority on cybercrime, terrorism, espionage, and so on. He speaks and consults worldwide. Power created the CSI/FBI Survey and his book Tangled Web is considered a must.

Dario Forte (www.dflabs.com) is one of the world's leading experts on Incident Management and Digital Forensic. A former Police Officer, he was a Keynote at the BlackHat conference and lecturer at many worldwide recognized conferences. He's also Professor at Milan University at Crema.