Proximal Consulting Archived White Papers

The Proximal Consulting white paper series began when Proximal Consulting launched in 1999. The white papers provided precise and detailed information on cutting edge business crime topics during a period when the Internet as a source of business information was in its infancy. We are now making these white papers available again.

Whilst the specific cases and examples used in the white papers are historical, the fundamental issues and potential red flags have remained the same.

Please note that the white papers are provided as an un-edited archive: any content, laws, regulations or similar were correct at the time of publishing, but may now be out of date.

PROXIMAL CONSULTING WHITE PAPER 6
DIGITAL & E-CRIME: WHAT YOU MUST DO TO CONTROL THE PROBLEM

One of the fundamental problems with IT security is that non-IT staff in organizations get completely tied up in knots about the systems and their attributes. IT staff talk in a language only understood by themselves - and non-IT staff in many cases either can't be bothered to make sense of it or don't ask their IT people to put it in language that can be understood. I've witnessed many organizations where the IT people have almost God like status and can't be questioned or doubted. The real crux of the matter is that to secure any IT system you only need to implement the kind of controls and defences that are (hopefully) already in place in every non-IT system or process. Perhaps I have maligned IT people too much....perhaps they don't think it's their job to make systems secure, perhaps no body has explained to them that their wonderful creations will attract the attentions of criminals...With all of these caveats these are the things you must do (now).....

- Test basic controls are operating effectively
- Have an up-to-date security policy
- Improve staff awareness on security issues - train and retrain
- Have a high level fraud prevention manager and define individual responsibilities for data security
- Use random mixed character passwords - they are much more effective than an English word. More importantly several software programs are available to search and isolate passwords that are dictionary and common names
- Don't forget Dumpster-diving and social engineering (which means in non American terminology that criminals will both steal your rubbish and try and con your staff to give out sensitive information by making pretext approaches)
- Vet potential staff
- Manage disgruntled employees
- Create a proper crime free environment - with the tone set from the top
- Employ risk analysis methods - what are your risks, what is the exposure and possible costs
- Segregate duties: separate application system analysis and programming, system programming, transaction authorization, file library maintenance and data control
- Job rotation
- Physical security controls - site planning, the control of access to restricted areas, protection of incoming supplies and outgoing material - which should of course all be cross shredded
- Access controls - mechanisms to identify authorized users, isolation features to close off areas of the system that users should be restricted from accessing
- Control hard copy data
- Encrypt sensitive data and e-mails
- Classify data: install and enforce an information protection policy
- Implement and test emergency response procedures
- Authorize inputs and transactions

- Design and implement exception reporting of any events which fall outside expected range - then make sure you act on the reports (and don't just file them/ignore them)

"The Internet opens the world. You don't have to be very sophisticated to do it. Nowadays everything is point and click"

- William Perez FBI acting section chief for financial crimes on hacking

SOME LESSONS THAT NEED TO BE LEARNT (quickly!)

- We can forget what happened in the last 1980 years - because what has happened in the last twenty years (probably in the last day) has seen more technological progress than in that whole period.
- Money can move anywhere, anytime in a keystroke
- Money loses its inherent value when it enters a computer - it becomes a line of code or a series of numbers in a vacuum. It only regains its value when it is stolen and converted somewhere in the world to hard currency
- The growing convergence and commonality of technology across the globe facilitates the transnational development of computer networks - this creates previously undreamt of opportunities for criminal misuse of them on a worldwide basis

Those criminal opportunities are already being seized which means that you could be hit at anytime in anyplace - and may not know it even when it has happened

November 2003 – Adapted from "Hacked, Attacked & Abused: Digital Crime Exposed" by Peter Lilley (Kogan Page, 2002)

Proximal Consulting

Email: enq@proximalconsulting.com

Telephone: +44 (0) 1672 516725

Offices:

Poughcombe Barns
Ogbourne St Andrew
Wiltshire
SN8 1SE
UK

Rue Du Rhone 14
1204-Genève
Switzerland

Proximal Consulting have unrivalled experience in providing KYC enhanced due diligence background reports on individuals and companies on a global basis. We also offer a complementary range of services including AML training, country risk reports and bespoke investigations.

Our enhanced due diligence reports are tailor-made to our clients' specifications. They are totally different from the usual database-led reports that often fail to meet enhanced due diligence requirements. Our reports present clear, accurate and confidential findings which enable our clients to make informed business decisions and to fulfil their AML obligations.

We work with a variety of global clients including regulatory agencies, law firms, individual companies, private banks, trust companies and other firms in the financial sector.
