I.T. and Security

Information security for smaller businesses

Colin Butcher
XDelta Limited

www.xdelta.co.uk
+44 117 904 8209

Personal background

- Systems architect specialising in mission critical systems
- Engineering background (printing, nuclear, energy)
- Software, operating systems, hardware, infrastructure
- Wide range of experience (utilities, aerospace, security, communications, finance, healthcare, transport, etc.)
- Started XDelta in 1996

XDelta – what we do

- Lead mission-critical systems projects
- Deliver world class services in demanding environments
- Strategic planning, technical leadership and project direction with clarity of vision and an eye for detail
- Systems engineering for availability and performance
- Ensure long term success through skills transfer

xdelta

Why does I.T. security matter ?

- Stay in business
- Avoid disruption
- Be safe – don’t lose data
- Be secure – don’t let others access your data

xdelta

Objectives

- Raise awareness – “constant vigilance”
- Reduce the FUD (fear, uncertainty and doubt)
- Understand more about the terminology
- Understand more about how things work
- Be better equipped to deal with problems

xdelta

Where are the problems ?

- People:
  - They lose things
  - They forget to do things
  - They expect things to be quick and easy
- Technology:
  - It’s complex
  - The language is arcane
  - It’s immature and evolving rapidly
- We need:
  - Protection against carelessness
  - Protection against malicious attackers

What is I.T. security ?

- It’s making sure that someone else doesn’t:
  - Steal or destroy your intellectual property
  - Get access to your data or systems
  - Get access to your clients data or systems
  - Stop you getting access to your data or systems
- What are the potential consequences ?
  - Damage to reputation
  - Disruption to your business
  - Disruption to your clients businesses
- How would you know if you’d been compromised ?

xdelta

I.T. security – the major issues

- Who takes responsibility for your security ?
- How can you recover from data loss ?
- Protection of information “at rest”
- Protection of information “in transit”
- Protection from external attacks
- Intrusion detection

xdelta

I.T. security – what can we do ?

- People are the weakest link, so help them understand the risks and how to deal with them
- Do the simple stuff well:
  - Lock the doors
  - Put equipment out of easy access
  - Don’t lose USB flash drives
  - E-mail is the least protected and biggest attack vector
  - “Phishing” attacks and “ransomware” cause more damage to smaller business than anything else
- Take frequent backups

xdelta

I.T. security – three key areas

- Authentication – are you who you say you are ?
- Access control – what are you allowed to look at / change ?
- Encryption – protecting information “at rest” and “in transit”

- It’s probably harder to protect a smaller business than a bigger business – why ?

xdelta

Threats

- Beware insiders – those you trust most can do the most damage to you
- Beware what you put in the public domain – consider the combination of pieces of information together with the opportunity and time for someone else to exploit them
- You only have to be a harder target than the others

xdelta

Threats: Information theft

- Identity theft
- Intellectual property
- Business knowledge
- Publishing private / secret material

Threats: Viruses and malware

- Viruses are generally carried by e-mail or other files being exchanged between computers (eg: USB flash drives)
- Be suspicious of e-mails from people you don’t know
- Never open attachments without scanning them
- Anti-virus software should be kept up to date
- The operating system should be kept up to date by applying security updates and patches

xdelta

Threats: Denial of service

- Flooding web sites with traffic to make them unresponsive
- Bombarding routers / firewalls to disrupt traffic flow
- “Ransomware” to block access to your files
- Bombarding systems to make them unresponsive or even crash the operating system
- Targeting specific equipment (eg: “stuxnet”)

xdelta

Information protection (1)

- Physical security
- Firewalls between your network and the Internet
- Anti-virus / software firewalls on machines
- Strong passwords
- Digital certificates
- Authentication devices (smart cards, RSA keys, etc.)
  - RSA = Rivest, Shamir and Adleman

Information protection (2)

- Encrypted network traffic:
  - Web site transactions (HTTPS)
  - E-mail send / receive (SSL / TLS)
  - Password protected / encrypted files (PDFs, ZIPs, etc.)
- Container file encryption
- Whole disc encryption
- Portable storage encryption

xdelta

Firewalls

- TCPIP V4 and TCPIP V6 protocol suites
- Allow / block TCP and UDP “ports”
- Allow / block addresses: senders / receivers
- Content inspection (but not encrypted content!)
- Hardware based – network-wide protection
- Software based – per machine protection

xdelta

Authentication and access control

- Strong passwords
- Single sign-on
- Windows Active Directory / LDAP (lightweight directory access protocol)
- Digital certificates

- *Comodo – one of many certificate providers*

xdelta

Encryption of data “at rest”

- File encryption
- Encrypted container files
- Whole disc encryption
- Drive based encryption

- *VeraCrypt (based on TrueCrypt) – Open Source (free)*

xdelta

Encryption of data “in transit”

- SSL / TLS (secure socket layer / transport layer security)
- HTTPS (hyper text transfer protocol secure)
- SFTP / SSH (secure file transfer protocol / secure shell)
- VPNs – used for remote access (virtual private networks)

xdelta

VPN connections

- Encrypted end to end path through network
- Linking small offices into a bigger network
- Remote access from anywhere
- Authentication: passwords, certificates, RSA keys, etc.

xdelta

Digital signatures and e-mail

- Digital signatures provide two key benefits:
  - Authentication of the sender
  - Encryption of the content (between two people)
- Why doesn't everyone use them ?
- *Comodo – one of many digital signature providers*

xdelta

Intrusion detection

- Firewall alerts and logs
- Anti-virus alerts and logs
- System event logs
- Can install audit software if needed
- Can set up additional controls such as ACLs (access control lists) if needed

Quick check-list (1)

- Think before you click!
- Anti-theft measures and physical security
- Carry copies of your data separately when travelling
- Send backup copies of files to a secure offsite location
- Encrypt and password protect files, especially portable media devices and offsite copies

xdelta

Quick check-list (2)

- Install and configure a hardware firewall and keep the software and configuration up to date
- Install anti-virus software and keep it up to date
- Install ad blockers and pop-up blockers in browsers
- Keep the operating system and software up to date

xdelta

Quick check-list (3)

- Use non-”administrator” accounts to log in
- Use PDF as a standard for interchange, not Word / Excel / Powerpoint / etc. files – why ?
- Never send personal data by e-mail, unless encrypted
- Anything you send by e-mail can be forwarded without your knowledge and after being decrypted

xdelta

Be secure (1)

- Protect all personal information
- Protect your clients information
- Regular backups of system and data
- Know how to restore backups
- Passwords – not all the same !

xdelta

Be secure (2)

- USB flash drives and other media – virus scanning
- E-mail – use whitelist / blacklist to control spam
- E-mail – attachment scanning
- Online banking – HTTPS, not HTTP
- Portable systems and media – use encryption
- Mobile devices – remote wipe if stolen / lost

xdelta

Be secure (3)

- Keep your business systems for business use only
- Be aware of what you put in the public domain
- Be aware of “data aggregation services” like Zoominfo and take ownership of your own data as best you can
- Screen your e-mail as you would phone calls and post
- Report incidents:
  - *www.actionfraud.police.uk* *0300 123 2040*

xdelta

Summary

- Make the effort to understand
- If something odd happens, don’t ignore it
- Think big, implement small
- Buy on functionality and reliability, not price
- Buy carefully from reputable suppliers
- Know who to go to for help
- Don’t be 100% dependent on technology

xdelta

Further information (1)

- ICO (Information Commissioners Office)
  - *https://ico.org.uk/for-organisations/guide-to-data-protection/*
  - *https://ico.org.uk/for-organisations/guidance-index/*

- UK Government, Dept. of Business Information and Skills
  - Publication “Small businesses: What you need to know about cyber security” – March 2015
  - *https://www.cyberstreetwise.com/it-policies*

- UK Government, Cyber Essentials scheme:
  - *https://www.gov.uk/government/publications/cyber-essentials-scheme-overview*

xdelta

Further information (2)

- IASME (Information Assurance for Small to Medium-sized Enterprises)
  - *https://www.iasme.co.uk/index.php/about*
- GCHQ – 10 steps to cyber security
  - *https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary*
- CERT (National Computer Emergency Response Team)
  - *https://www.cert.gov.uk/what-we-do/*
- FCC (Federal Communications Commission - USA)
  - *https://www.fcc.gov/cyberforsmallbiz*

xdelta

I.T. and Security

Information security for smaller businesses

Colin Butcher
XDelta Limited

www.xdelta.co.uk
+44 117 904 8209