



CYBER SECURITY

SUPERHERO SERIES 2012

Join the fight against cyber crime!

Cisco | Networking Academy®
Mind Wide Open™

Domenic Seibold
Security Specialist
Cisco



About me



Domenic Seibold

My journey is 16+ years and counting - from play to practice to design to the business of...

It's all about what you do with the data, just collecting it is not enough – that's what defines...

Everyone is responsible for...

Security

It's what you do with it...

Successful security practitioners constantly review the process, the people and the data

Always question what you are doing.

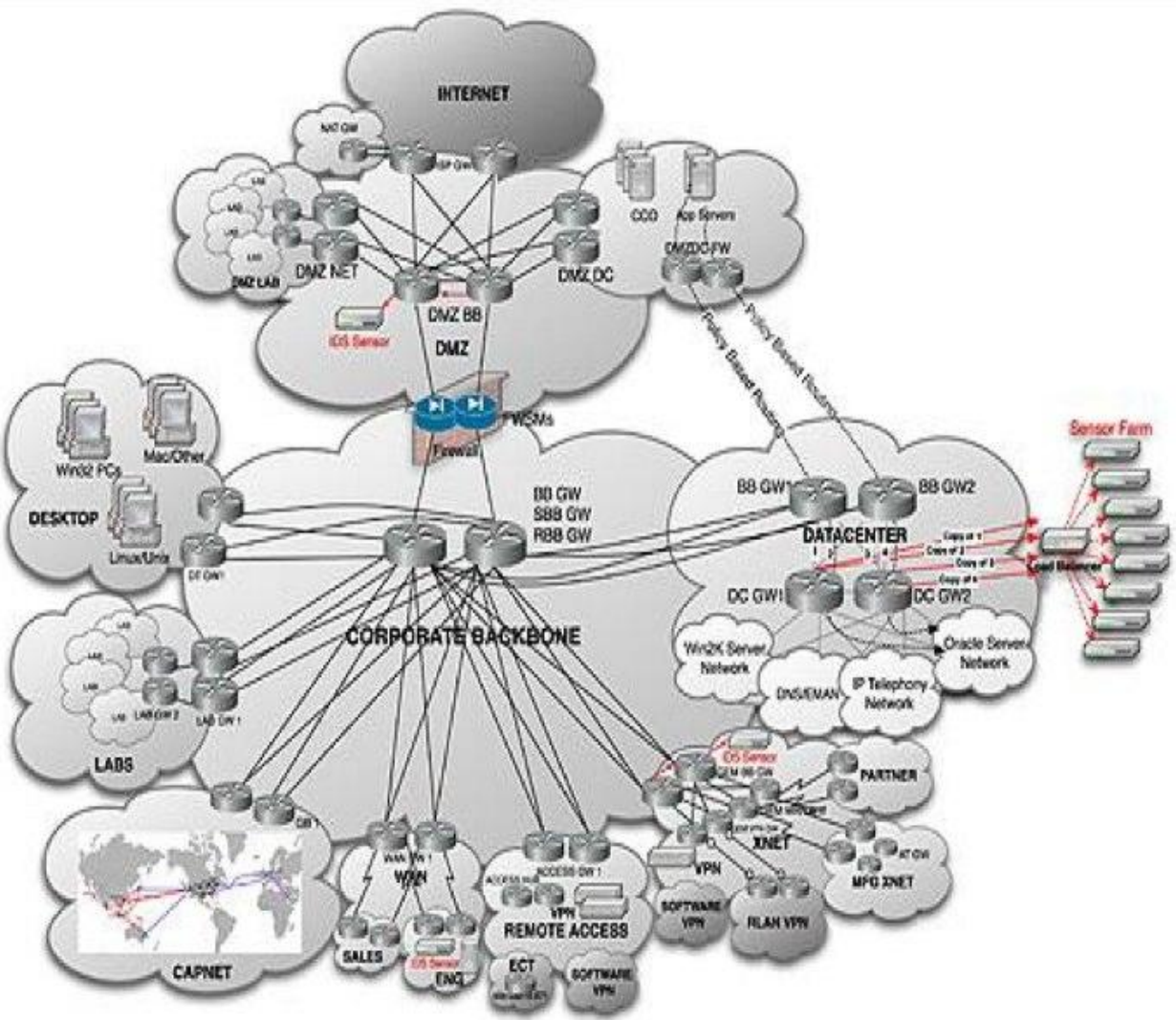
You get what you measure.

Shamelessly copy from someone else.



Technology and Users are not the Problem

Complexity Is



IPv6

- 3ffe:1900:4545:3:200:f8ff:fe21:67cf or
- fe80:0:0:0:200:f8ff:fe21:67cf or
- fe80::200:f8ff:fe21:67cf

Tunneling

- Router-to-router
- Router-to-host
- Host-to-router
- Host-to-host
- Multi-homing

Mobile Ad-Hoc Networks

- Mesh
- Wireless
- Vehicle MANET
- Intelligent vehicle MANET
- Internet-based MANET

Miniaturization

Multi-Purpose Devices

Eradication of Perimeters

- Partners, customers, government, competitors, public

Virtualization

Cloud Computing

See, Don't Feel – Analyze

Data Removes Emotion

Understanding /
Strategy /
Action

Hosting

Net Team

SecOps

Others

Information

Event /
Behavior
Correlation

Network Analysis

System Analysis

Security Vendor

Others

Identity

Geo
Location

Proximity

Homegrown
Apps

Data

Sensor
Logs

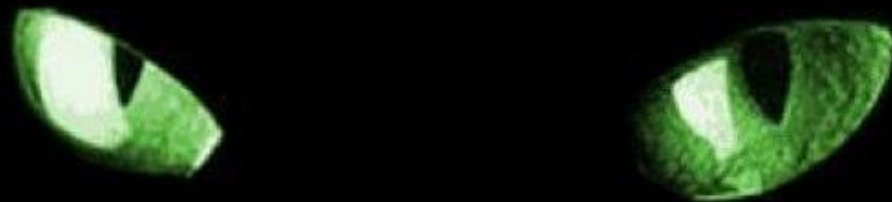
SCADA

Others

“I have a series of questions, and the data gives the answers”

~ or ~

“I don't know the questions yet; let's look at the data”



Our adversary only has to be right once...

We need to be one step ahead
and always on top of our game





Thomas Lenzenhofer
Security Network Consulting Engineer
Cisco

About me



Thomas
Lenzenhofer

- Born in Vienna / Austria
- Engineering Degree in Telecommunications.
- 1993-1997: Network support & implementation field engineer for Austrian Network Integrator company.
- 1997-2000: Senior Network Support Engineer for Bay Networks/Nortel in EMEA HQ/South France.
- 2000-2003: Senior Network Support Engineer for Cisco Systems APAC/Sydney/Australia.
- 2003-current: Working as Security Network Consulting Engineer for Cisco Systems.



What I do at Cisco?

- Part of the Worldwide Borderless Network Practice in the Advanced Services team with a focus on Network Security.
- Responsible for Cisco Network Security Architecture Review, Solution Design and Implementation within the large Enterprise and Service Provider market throughout Asia Pacific, Australia and New Zealand. Occasionally in other global regions.



Key Engagements in the last 10 years

- Security Design and Implementation for Malaysian International Airport and Government Agency.
- Various Security Designs and Implementations in Australia such as for Australian airline, retailer, university, banks and service providers.
- Security Architecture Review for Banks in Australia, Philippines and China.
- Security Consulting Services for China's largest travel agency and bank in preparation for Beijing Olympics.
- Various Security Design and Implementation engagements throughout Asia such as new R&D facility for world's largest notebook manufacturer in Taiwan, Asian Stock Exchange, Service Provider in Thailand, Philippines, China and Hong Kong.
- Large Datacentre Security Designs and Implementation for Australian retailer and Government



Why Network Security?

- Almost all companies today, whether small or large, run their business over a network and connect to the Internet. The business would not function without the network.
- Human interaction - whether for business, personal or other reasons – increasingly relies on networking and the Internet. Large societies are built on these networks and it became part of people's life's to connect in these ways.
- Whether for business or personal reasons – the Internet and network is now an integral part of almost everyone's life. People put a lot of trust into the network to be there for them and provide what they need – a trust that others with malicious intent abuse.
- Network Security is now an essential element to anything related to networking and its importance is in direct relation to the importance and reliance people place on the network. The more we rely on the network, the more important Security becomes as there will always be some bad guys out there.



What you can expect

- A profession/job that gets never boring. There is enormous variety out there, even though it all falls under Network Security.
- Be realistic and set the right expectations – you will never win. Nothing is 100% secure unless you disconnect it and power it down. What can be secured can be broken or circumvented. It is an arms race with the bad guys. On the upside, this also means good job security and it's a useful profession trying to make the Internet a better place.
- As everything in this world and certainly the IT industry – things constantly change. This means constant learning and adjusting but with this also comes great variety – which keeps it interesting in the long term.



The banner features a central figure of a person in a black trench coat and hat, holding a padlock with a yellow and black hazard stripe. To the left is a shield with a yellow and black chevron pattern. The text 'CYBER SECURITY' is written in large, metallic, 3D letters. To the right, 'SUPERHERO SERIES 2012' is written in a smaller, blue font. Below the main text, a white bar contains the text 'Join the fight against cyber crime!'. At the bottom of the banner, there is a row of small icons: a skull, a red face, a horse, a computer monitor with a green checkmark, a brick, a hand holding a brick, a hard drive, and a broom. The Cisco logo is in the bottom right corner of the banner.

CYBER SECURITY SUPERHERO SERIES 2012

Join the fight against cyber crime!

Cisco | Networking Academy®
Mind Wide Open™



Simon Finn
Senior Security Architect
Cisco



About me



Simon Finn

18+ years of Security : Worked
in all aspects of Information
Security

Solving complex business
problems whilst lowering risk

It all started in engineering...

Desire to know how stuff works?

- Curiosity is a strong driver
- “Hacking” originated through wanting to know more, but has become its own industry
- Security professional have to have the similar knowledge or the battle is lost

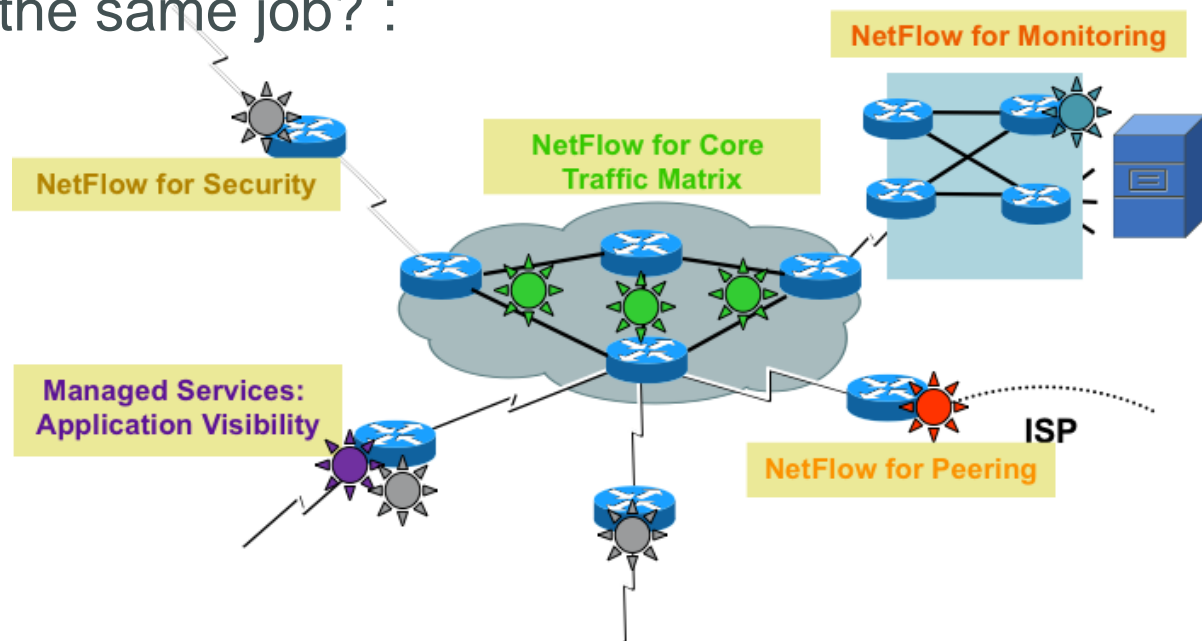


“The mantra of any good security engineer is: 'Security is not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.”

— Bruce Schneier

“Defense in Depth”

- Breadth and depth... of knowledge
- Every layer is secured, every node of every system
- Data must be secure at all stages
- More than one tool for the same job? :
 - Arbor
 - Lancope
 - NetQoS



“The user's going to pick dancing pigs over security every time.”

— Bruce Schneier

The network is at the forefront of modern enterprise security



- “Borderless”
- “BYOD”
- Virtualisation/
Cloud



The banner features a central figure of a superhero in a black suit and hat, holding a shield with a yellow and black chevron pattern. To the right, the words "CYBER SECURITY" are written in large, metallic, 3D block letters. Above "SECURITY", the text "SUPERHERO SERIES 2012" is written in a smaller, blue font. Below the main text, a white banner contains the text "Join the fight against cyber crime!". At the bottom of the banner, there is a row of icons: a green skull, a red and orange flame, a horse, a computer monitor with a green checkmark, a brick, and a white hard drive. To the right of the icons is the Cisco Networking Academy logo and the slogan "Mind Wide Open™". The Cisco logo is also present in the bottom right corner of the banner.

CYBER SECURITY SUPERHERO SERIES 2012

Join the fight against cyber crime!

Cisco | Networking Academy®
Mind Wide Open™



Colin Bradley
Chief Security Advisor & ANZ Channels Lead
Asia Pacific, Cisco

About me



Colin Bradley

- Born in Birmingham, UK
- Maths and Science at 'A' Level
- BA Hons Degree in Business Studies (with a specialisation in Marketing) – included a 12 month placement with IBM UK.
- 1987 – 1993: Sales Executive, Harris Systems
- 1993 – 1996: Sales Executive, Firefox and other software solutions vendors.
- 1996 – 2003 Sales Director / Managing Director, Harrier Group plc (a security systems integration business)
- 2004 – 2006 Security Practice Manager, Dimension Data UK
- 2006 – to date Security BDM / Security Advisor, Cisco Systems in Sydney, Australia



What I do at Cisco?

- Part of the APJC Borderless Networks Team with a focus on Network Security for Service Provider segment and BN Architecture for Principle GTM Partners.
- Responsible for developing relationships with BN and Security Practices in selected Cisco ANZ Gold Partners and for building Executive level relationships, and relevance, with customers in the SP segment (eg. Telstra, Optus-AW, VHA etc.) and with key transformational accounts (eg. ANZ Bank, NAB etc.).



Key Engagements in the last 5 years

- Represent Cisco on the ITSEAG (part of the TISN)
- Working as part of Telstra “Project Enterprise” and on new architectures for the deployment of appropriate project related security controls – especially in Cloud.
- Leading the engagement at NBNCo to build out an effective DC perimeter and to engage on security architecture so that Cisco is relevant to such an important nation building project
- Worked as part of the CAC to establish a new Bachelor of IT degree course in Network Security at NSI – North Sydney.

What about the Future? Growth Opportunity or Threat?



Is Device Proliferation a Security Challenge?

- Over half of IT leaders believe employee-owned mobile devices pose greater risk
- Threats include:
 - Difficult to control and secure
 - New Malware variants
 - Data loss from lost or stolen devices
 - Data leakage
 - Access control breach
 - Maintaining policy compliance



It's no longer possible to remain secure!

Three types of organisation now exist:

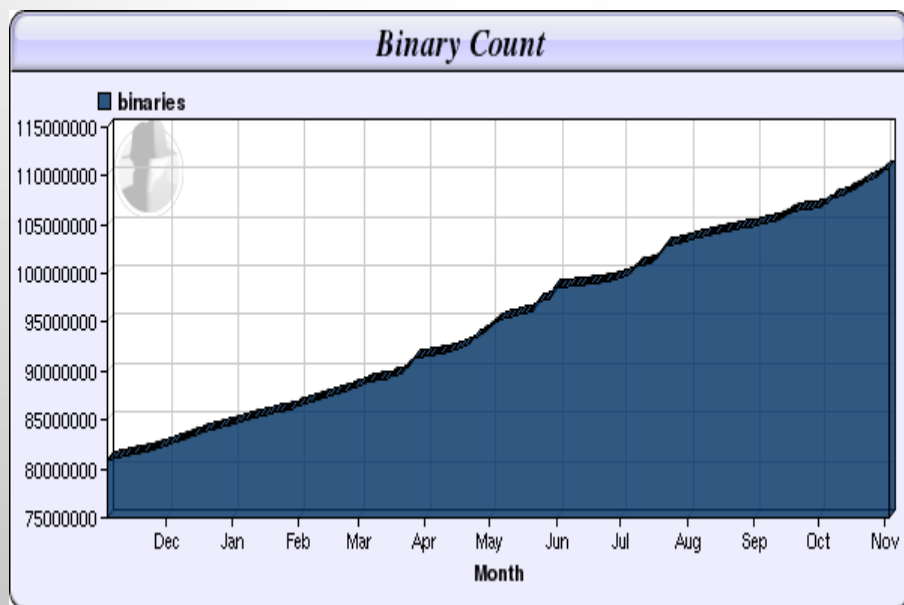
- 1) One that has been compromised
- 2) One that has been compromised but isn't aware of it yet
- 3) One that is about to be compromised

Hence, it's all about degrees of insecurity...

So, where to next?

The Definition of Insanity.....

Do we just keep on doing the same old things?



www.shadowserver.org/
4 November 2011
~38 million new hashed binaries in the past year; ~111 million total seen

So, what should we focus on?

- 1) Get back to basics – do less well
- 2) Sharing: Illuminate problems and ideas publicly
- 3) Know what you are protecting and what condition it's in real-time
- 4) Instrument for detection and choose someone help watch over you
- 5) Measure effectiveness



Thomas
Lenzenhofer



Domenic
Seibold



Simon
Finn



Colin
Bradley

Panel discussion A day in the life of a Cisco Security Expert

Thank you.

