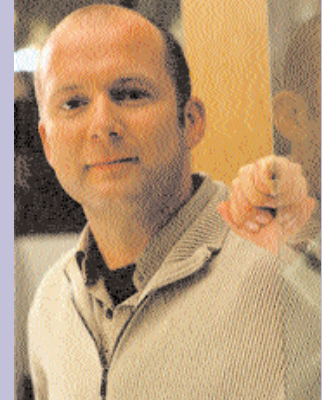


By Kevin Whelan, Technical Director
ITC Network Services Limited
k.whelan@itc-network.com

Network Security in a Dangerous World

7 Steps to Securing your Network



Learn how to:

- Take control of your network security
- Assess risk
- Implement a rock solid security policy
- Implement an early warning system you can count on
- Choose the right VPN and Firewall solution to protect your organisation

Who should read this:

- IT Managers and Directors
- Network Security Managers
- IT Professionals
- Business Managers

Introduction

In this white paper 7 Steps have been outlined to help you secure your network. These are practical steps designed specifically for those who are responsible for their organisation's network or network security and are relevant to all types and sizes of organisation.

The human aspect is critical to any security strategy: if people haven't been trained to be secure, then the chances are that they won't be secure. A rigorous training and re-training strategy is required; technology alone will not suffice. (This is covered in Step 6 – Educate your staff.)

Many organisations think that they are 'secure' because they have a firewall to protect them from intrusion via the Internet - this is far from the truth. Think about the inside of your network. It may be prudent to think of protecting your internal servers with additional firewalls or authentication. If somebody really wants to get the information, it could be far easier for him or her to get a job at your organisation and do it from the inside.

BS 7799, the standard for information security, is also highly relevant, but covers aspects outside the scope of this white paper, for example, paper based information. Understanding BS 7799 and how it is relevant to your organisation is also highly recommended reading.

The Turnbull Report on Corporate Governance has highlighted how absolutely crucial the 'adoption of a risk-based approach to establishing a system of internal control and reviewing it's effectiveness' is to running a successful business. The lessons from Turnbull are applicable directly to how IT security is implemented and administered within an organisation. 'Implementing Turnbull – A Boardroom Briefing' (www.icaew.co.uk) is strongly recommended reading in conjunction with this White Paper.

Do think about this white paper and see if any of its tips can assist you in your security strategy. Of course, if you have any questions about this white paper, I'd be happy to answer them. Please email them to k.whelan@itc-network.com.

Kevin Whelan
Technical Director
ITC Network Services
London, England.

Attack and Defence

Five ways you can be attacked (and possibly destroyed)

1 Denial of service attacks

2 Hackers

3 Insiders

4 Physical break-ins

5 Viruses

Eight ways to defend yourself

1 Training of the organisations staff

2 Anti virus software

3 Authentication

4 Firewalls

5 Intrusion Detection Systems (IDS)

6 Public Key Infrastructure

7 Virtual Private Networks (VPNs)

8 Physical security

Step 1

Create and publish a Security Policy

This is where top management set a clear strategy and demonstrate their commitment to Information Security.

Ask yourself this question: “Is there a formal information Security Policy in my organisation?” If the answer is “no” then the chances are that your organisation does not have a clear defined strategy on how to keep it’s network secure.

The objective of developing a security policy is to achieve top-level support and control of information protection. To achieve this, top management must participate in the creation and operation of a clear information protection policy across the organisation.

Your Security Policy should complement the organisation’s ‘mission’ statement and reflect the desire of the business to operate in a controlled and secure manner.

As a minimum the Security Policy should include guidance on the following areas:

- The importance of information security to the business process.
- A statement from top management supporting the goals and principles of information security.
- Specific statements indicating minimum standards and compliance requirements for:
 - Legal, regulatory and contractual obligations
 - Security awareness and educational requirements
 - Virus prevention and detection
 - Business continuity planning.
- Definitions of responsibilities and accountabilities for information security.
- Details of the process for reporting suspected security incidents.

Every staff member needs to have the policy explained in detail (don’t just email it to everyone and hope they read and understand it). As security is fundamental to operations, the policy should also be displayed in public places. ‘Refreshers’ every 3–6 months to remind everybody of their responsibility are also crucial.

Step 2

Create guidelines

You need to decide how your organisation will be responsible for implementing security.

The support of the Chairman or Managing Director of your organisation will probably be the most effective way to get the job done. As with any project, not having the support of senior management means the project will fail. You cannot afford to let this happen.

If your organisation is big enough, it may have its own 'Information Security Manager'. In a smaller group, the IT Manager or other senior manager may assume this role on top of their existing one.

You need to be very clear in specifying what and how often procedures or policies need to be reviewed. Usually this happens when something changes. For example: you may have a web server hosted externally at an ISP. You then decide to bring it in-house, effectively as part of your LAN. Another example may be when a senior IT person with multiple 'administrator' rights to different systems leaves his job, or, perhaps your company merges with another company.

All security roles should be clearly defined within a job description so that there are NO grey areas as to who has responsibility over what.

For example, a section of an Information Security Manager's job description might read:

"It is your responsibility to ensure that ABC Limited does not suffer from network propagated, or otherwise propagated, known viruses. ABC Limited has an agreement with Antivirus Software PLC and the latest anti-virus update or patch is installed onto every PC with ABC Limited. Company policy is to check at least twice a day with the Anti Virus manufacturer that ABC Limited has the latest version. It is also your responsibility to ensure that ABC Limited has the best and most effective means of virus defence."

Step 3

Assess your risk

Assessing the risk throughout your organisation involves identifying each 'asset' and assigning a level of risk to it.

You can define risk as 'what would happen to my business if I lost this asset?' You could define loss in monetary terms, customer satisfaction, and inconvenience or in any way that describes the impact of losing an asset.

For example, say you had two servers:

1. The first had your corporate database with the entire history of all of your clients' purchases (including correspondence between you and them), payroll data and future product releases.
2. The second was used to house the intranet, carrying lots of useful information, but nothing mission critical.

Security measures should be justifiable, practical and necessary. They should be balanced against the business risk of disclosure. Business risk is assessed in the following terms.

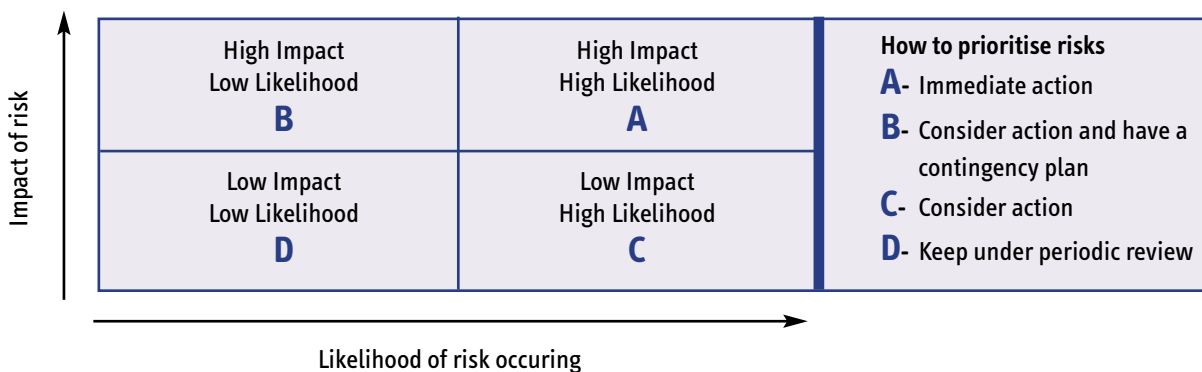
If you had to assign a risk value to both of these servers, the chances are that you would identify Server 1 as the one that would have the biggest impact on your business if you lost the server and the information on it. (Generally speaking, the information is worth far more than the actual equipment it sits on.)

Your results will tell you exactly what needs to be secured, what type of security is appropriate (e.g. anti-virus, firewall, VPN), how strong the security needs to be, how quickly you need to get it done, who is responsible for it, what policy is to be applied to the security and how often it needs to be reviewed.

Continue to do this for every 'asset' in your organisation.

(For an in-depth guide to Risk Assessment go to www.bsi.org.uk)

A risk matrix below should help you prioritise your risks.



Step 4

Implement security standards

A security standard will help you choose the right security measure for a specific scenario.

Having assessed the risk for each part of your network (including people!), apply the following rules to high priority items first, then medium risk and then low risk.

1. What type of security is appropriate (e.g. anti-virus, firewall, VPN).
2. How strong the security needs to be.
3. How quickly you need to get it done.
4. Who is responsible for it.
5. What policy is to be applied to the security measure and how often it needs to be reviewed.
6. What level of risk the asset is.
7. Compliance with the Data Protection legislation.

Step 5

Business Continuity

The objective is to have plans available to counteract interruptions to business activities.

Business Continuity plans should be available to protect critical business processes from the effects of major failures or disasters.

'Business Continuity' is the term applied to how a business would continue to operate after a business 'interruption'. The term 'interruption' can mean anything from a key member of staff being off sick right through to the outbreak of war. Fail to cater for unexpected 'interruption' and you should expect to pay the price. This could mean total business failure in extreme cases.

Knowing what to plan for should be directly tied to [Step 3 'Assess your risk'](#). By looking at your risk assessment process, the Grade A 'High Impact, High Risk' will be needed most to continue operations whereas Grade D 'Low Impact, Low Risk' items are less likely to be needed. (This begs the question: if it is not needed for business continuity, is it needed at all? That, however, is another discussion.)

Business Continuity Planning Process should be a managed process in place for developing and maintaining business continuity plans across the organisation. Do you have a business continuity planning process? What is it? Who is in charge of it? How is it managed?

Business Continuity Planning Framework should be a consistent guideline to be applied to your plans.

Testing Business Continuity Plans is critical to finding out if they work or not. Everything may sound OK in theory – but does the plan actually work. For example, if your email server database gets corrupted, do you know for a fact that the back up server will work?

Updating Business Continuity Plans should happen periodically or whenever changes to your IT systems happen. For example, when your organisation moves location and implements a new infrastructure.

Simple and powerful ways to protect your organisation in the event of an interruption are:

1. Mirror your central IT systems onto identical systems situated at another location or data centre. Connect these systems using a VPN back to your office. In the event of your normal IT systems failing, you have a system ready to go.
2. Investigate the possibility of permanently locating your central IT systems into an outsourced (or your own) data centre, with a back up system at another data centre and then accessing those systems via the Internet. A purpose built data centre has many advantages over a typical data room inside an office.
3. Have a complete and accurate paper based record of your IT systems, including the nature of the information it stores, and how the business uses the systems. This should be stored on-site as well as off-site (in a secure facility). If, God forbid, everything is lost, you will still have a way of rebuilding your systems.
4. Make sure that your team are correctly trained on:
 - a. How to identify and categorise an interruption.
 - b. How to work out what impact the interruption will have on the business.
 - c. What to do to minimise or negate the impact.
 - d. How to restore normal service (of course this could involve many people throughout the organisation based on the impact of the interruption).
 - e. How to log the nature of the interruption, lesson learned and solutions as how to stop this from happening again.
5. Educating staff continually as to the importance of backing up files properly onto back up servers and using proper security measures at all times, such as virus checking and changing passwords. (Prevention is better than cure.)
6. Making sure ALL staff know exactly what to do in the event of a business interruption.

Step 6

Educate your staff

In the introduction, we stressed the importance of people in the security process. You can have the strongest and most robust lock in the world, but if you don't shut the door, you're not secure.

According to the UK Department of Trade and Industry, in well over 90% of organisations there is no formal training or education process to teach staff on how to be secure. If you want to instantly avoid this critical security flaw, then start by implementing a corporate security-training program. Outside consultancies can do this for you, too. An emailed memo on 'How to be secure' WILL NOT suffice!

Training should include

1. What security means.
2. A summary of The Ten Key Controls of BS 7799 and how they affect a business.
3. An outline of why the organisation and each staff member needs to follow security procedures.
4. What could happen if they don't?
5. A detailed explanation of the organisation's Security Policy (see Step 1) and how it affects them.
6. How to report security breaches (and the importance of reporting them)
7. Business Continuity procedures.
8. An opportunity for staff to make suggestions and review earlier ones.

Every staff member should have security training sessions at least every 6 months. It is paramount that the Board and senior Directors are highly visible at the sessions to demonstrate how seriously the organisation takes security.

Information should be easily accessible via your Intranet and IT support staff should take advantage of the personal relationships they develop with the people they support to teach security. This method means that the organisation is in a continual state of teaching and learning. This is the best way to stay secure.

Step 7

Check for compliance

You need to make sure that your systems (people as well as technical) are working properly and that full assurance can be given to the board that effective measures are being taken to mitigate security risk.

Compliance is carried out by way of an internal or external outsourced audit. An audit checks that:

1. Procedures match security policy.
2. Security policy reflects risks within the organisation.
3. Technical devices (firewalls, virus scanning, intrusion detection etc) are suitable, in working order, have the correct policies applied, are situated correctly and are licensed properly.
4. Procedures and policy are followed properly by staff.
5. Any possible threats are identified clearly, with corrective measures specified.

Corporate IT security is incomplete without an effective audit. Auditing will highlight areas within your IT systems that are prone to vulnerability.

For listed companies in the UK, the advent of the Turnbull Report and Combined Code on Corporate Governance means that if companies do not check for compliance and sign-off appropriately in the end-of-year accounts, the value of the company could be negatively affected. There are real, bottom-line implications for non-compliance.

Risk management

Three risk management facts you need to know

- 1** Over 90% of all security threats come from WITHIN your organisation.
There is an automatic assumption that if a firewall is up and running there are no further issues to worry about. Wrong. Staff can load floppies and CD's onto their computers (as well as download from the Internet). Are you confident that each and every machine can rely on itself to detect a virus? Is the anti-virus software up to date with the latest patches?

How about the modem on Mike from internal support's PC? Could someone dial into that and access your network?

The largest threat is the failure of people in organisations keeping on top of the security issue.

- 2** Over 80% of all firewalls have out of date patches installed or are incorrectly set-up.

Really? Absolutely. To ensure your firewall is up to date you have to keep it fresh with the latest patches from the manufacturer. If you don't, you are destroying what the firewall is supposed to be doing. Make sure that your firewall has the latest software from the manufacturer.

- 3** You can never eliminate risk.

Choosing the right firewall & VPN

Shopping for an enterprise firewall can be intimidating if you've never done it before. However, with a little background knowledge, an understanding of firewall features, and knowing what questions to ask the vendors will help you to source the right firewall for your organisation.

Types of firewalls

One of the first things you need to figure out is what type of firewall best suits your needs.

There are six basic types of firewalls:

1. Embedded firewalls
2. Enterprise software-based firewalls
3. Enterprise hardware-based firewalls
4. SOHO software firewalls
5. SOHO hardware firewalls
6. Speciality firewalls

All of these firewall types typically offer stateful packet inspection or proxy capabilities. Stateful packet inspection and the ability to proxy are different techniques that firewalls use to make decisions on what traffic to allow or deny into and out of your intranet. While in the early days of firewall development most firewalls offered either one or the other of these types of traffic passing architectures, today, leading firewalls with hybrid architectures offer both techniques to secure your intranet traffic.

Stateful packet inspection firewalls examine protocol packet header fields while proxy firewalls filter services at the application level. Stateful packet inspection firewalls learn and remember connection states and evaluate new traffic transactions against prior connection histories. Proxy firewalls are able to create virtual connections and can hide the internal client IP address making it more difficult to discern the topology of the protected intranet.

Firewall Types Explained

Embedded firewalls are firewalls that are embedded into either a router or a switch. Sometimes embedded firewalls come standard with certain routers, and other times you can purchase an add-on firewall module to install into a router or switch that you already have. Embedded firewalls are sometimes referred to as choke-point firewalls.

Due to the wide variety of different protocols used on the Internet, not all services are handled efficiently by embedded firewalls. Because embedded firewalls work at the IP level, they will not be able to protect your network from application level exploits such as viruses, worms, and Trojan horse programs. In some cases, embedded firewalls might offer greater performance gains, but they typically offer fewer features for protecting your networks. Embedded firewalls are often stateless in nature, and pass packets without consideration of prior connection states.

Software based firewalls are software packages containing firewall software that you install on top of an existing operating system and hardware platform. If you have a server with an enterprise class operating system that is available for use, purchasing a software-based firewall is a reasonable choice. Also, if you are a small organisation, and want to combine a firewall with another application server (such as your web site server), adding on a software-based firewall is reasonable. If you are a large organisation, you will probably want to create a security perimeter network known as a DMZ (demilitarised zone) and will therefore want to separate your firewall from all other applications. Software-based firewalls come in both small office/home office (SOHO) models and enterprise models.

Hardware-based firewalls are the same thing as appliance firewalls. The entire firewall is bundled into a turnkey system and when you buy it, you get a hardware device that has the software already inside it. Hardware-based firewalls, or appliance firewalls, also come in both SOHO and enterprise models.

Speciality firewalls are firewalls with a certain application focus. For example, there are some security servers with built-in firewall-type rules that are made particularly for filtering content, or security messaging servers. As security technologies become more advanced, sometimes the product segments start to blur and you need to understand what the product actually does, and not rely on its vendor marketed product definition.

Users, Locations, and Numbers

A consideration that should be very high on your list is how many users do you need to protect, and how many firewalls will you need? The number of users you are going to protect will determine whether you need an enterprise class firewall or a SOHO firewall. (You can certainly use an enterprise firewall, even for one user, but you might be paying a lot more than you need to pay, and might end up with features you will never use.)

Most SOHO firewalls can accommodate enough connection requests for up to 50 users. If you plan on protecting more than 50 users with your firewall, it's time to move up to an enterprise firewall. SOHO firewalls typically range in price from £30 to £1000. The £30 firewalls are typically used for one person, one system. A £1000 SOHO firewall is sufficient for a small field office of less than 50 people.

Enterprise firewalls, typically ranging in price from £500 to £20,000 and more, are commonly used in organisations that require multiple firewalls that need to be managed from one location. This means that enterprise firewalls need to be able to communicate with some sort of central management console. Most vendors who make enterprise firewalls offer a central management console as an option.

Alternatively, there is a young and growing security market segment of Security Information Management (SIM) devices that can essentially be used as third-party management consoles. Both netForensics and e-Security make third-party SIMs that can integrate with various leading enterprise firewalls.

Depending on how you design your security perimeter network and how much money you are able to spend, one robust firewall on your perimeter may be sufficient for your organisation's needs. The important thing is to ask the vendors you are interviewing how many users each firewall can support. Most reputable firewall vendors rate their firewalls for a certain range of user connections. Typically the more users you need to support, the more RAM and processing power you will need in your firewall.

A sizing guide that will apply to most reputable firewall vendors is found in the table below. Note that the RAM listed in the table is what the firewall itself requires. If you have other applications running on your firewall system, you will have to take into account this amount of RAM, on top of what your other applications require.

If you plan on pumping streaming media through your firewall, or plan on using a VPN, both of these applications can benefit from more processing power, and more RAM.

Number of Users	RAM Needed by Firewall	Processing Power	# of Offices	Packet Filter Throughput	Price Range
Under 50 (SOHO)	Less than 10 mb	~ 66 Mhz	1	Less than 10 Mbps	Less than £500.00
51-1000	65 mb	~ 200 Mhz	2-299	Less than 100 Mbps	Approx £5,000.00
1001-5000	128 mb	~ 500 Mhz	300	Less than 200 Mbps	Approx £ 10,000.00
Over 5000	256 mb	~ 500 Mhz +	Over 300	Over 200 Mbps	Approx £20,000.00

The Trade-Offs

Software firewalls offer more flexibility than appliance firewalls; because you can choose what hardware platform you want to run the firewall on. However, having to make a decision on what hardware platform and operating system to build your firewall on, is a decision that some information technology managers and engineers do not have time to make. If the concept of "I don't care what type of hardware platform the firewall runs on as long as it works," appeals to you, then an appliance firewall might be preferable. With an appliance firewall, you get a complete turnkey firewall bundled into one box. Because there are less procurement decisions to make and everything comes pre-packaged as much as possible, getting an appliance firewall up and running usually is much faster than getting a software firewall up and running.

In most cases, unless you are using a speciality firewall, you will want to separate your firewall services and not install your firewall on top of other applications.

NAT

Today, almost all leading firewalls come bundled with network address translation (NAT) capabilities. However, there are different categories of NAT that you might want to be aware of. NAT gives you the ability to translate private or illegal IP addresses into legal public addresses and, as an aside, it helps to hide the internal topology of your network(s).

There are four types of NAT configurations to be aware of: one-to-one addressing, many-to-one addressing, one-to-many addressing, and many-to-many addressing.

The one-to-one NAT configuration is the most basic of all NAT features. This feature maps an internal IP address to a different external public IP address. Many-to-one addressing means that multiple internal IP addresses can be mapped to one external IP address. You might want to do this if you have an internal DHCP scope that you want to map to one external IP address. Many-to-many NAT addressing is for mapping groups of internal or external IP addresses with different groups of IP addresses on other networks. You may want to use many-to-many NAT addressing if you are mapping one set of DHCP scopes to another. A one-to-many NAT scenario is most commonly used in load-balancing scenarios where you want to take one IP address, and split it into two. If you have a big and complex carrier-class network you will want advanced NAT features. For SOHO networks simple one-to-one NAT capabilities are probably sufficient.

VPN Capabilities

Firewalls are commonly used as VPN endpoints, and some firewalls offer VPN capabilities. VPNs allow you to use site-to-site encryption. While a firewall acts like a road-block, and only lets certain traffic in and out, once the traffic is out on the Internet, it is being transported in clear-text, and with a sniffer, is viewable to the world. The only way to ensure privacy and data integrity is to use a VPN. If you decide you need a VPN, keep in

mind that a VPN implies two endpoints. There is no point in getting a VPN if you don't have a second endpoint to connect it to because a VPN does not work with only one endpoint.

VPNs send your data through an encrypted tunnel, keeping it private from the rest of the world. The encryption process requires additional processing power, and if you are setting up a VPN for a carrier-class network, you will need one that either comes bundled with a crypto accelerator, or allows you to add-on a crypto accelerator. Crypto accelerators take slow VPNs and make them faster.

Logging

Logging capabilities is one of the most important features of any firewall, and not all firewalls log events equally. You want a firewall that can log as many different types of events as possible, and can filter on as many different types of events as possible. So one question you will want to ask a prospective firewall vendor is how many different event types a potential firewall can log, and how many different filters the logging capability has. The filters allow you to view the different events in a logical and understandable way. For example, you should be able to filter on events by things such as IP address, network numbers, connection types, domain names, and by date and time (to name a few basic filters). The Syslog format is the most commonly used logging format, and if a particular firewall does not support Syslog, you might want to think about crossing it off your short list.

Firewall Rules

The firewall rules and the definitions you set up which tell the firewall what types of traffic to let in and out of your network. All firewalls have a rules file and it is the most important configuration file on your firewall. An important question to ask your prospective firewall vendor is whether you will need to reboot the firewall every time you make a change to the rules file. If you are shopping for a carrier-class firewall this is a must. If you are in the market for a SOHO firewall, an occasional firewall reboot will probably not impact you too much.

Another feature to find out about is if the firewall supports automatic order-independent rules. The rules on a firewall need to be in a very specific order or they will not work properly. Some firewalls have the ability to order the rules automatically. This feature can be both good and bad so you will want to make sure that if it exists, there exists the capability to turn it on and off. The algorithms and code used to make the order-independent rule setting decisions need to be completely bug free, or using this feature could open up security holes on your network. In a perfect technical world, automatic order-independent rule setting is a great feature because if you have a lot of firewall rules, it can help you understand how to order the rules properly. However, there is no substitute for human knowledge in setting up your firewall rules.

Summing it all up

There are more things to know about firewalls beyond those I have discussed here, but hopefully this will be enough to get you going. Other features you might want to research are high-availability, content filters, and the ability to support anti-virus features. Before you start talking to firewall vendors, make a list of questions that you want to ask each vendor. Ask all the vendors the same questions, and refine your list as you talk to more vendors. Be sure to ask them about their phone support and management packages, and if this is included in the license fee. Good firewall phone support as well as online management is key to helping you become comfortable and proficient at configuring your new security device.

About ITC Group

Contact Details

ITC NETWORK GROUP LIMITED

14 Jessop Square
Heron Quays
Canary Wharf
London E14 4JB
UNITED KINGDOM

Tel: 0800 107 7712

Int: +44 (020) 7517 3911

Fax: +44 (020) 7515 4542

Email: sales@itc-network.com

About the Author

Kevin Whelan has specialised in network design and security for over 20 years. He was responsible for the integration of the 170,000 user Price Waterhouse and Coopers and Lybrand networks after the firms merged. Kevin is also security consultant to a consortia of the world's leading banks as well as many corporations in the UK and around the world.

Kevin is a graduate of Kingston-upon-Thames University in Surrey, England, is married with a son and thoroughly enjoys talking shop over a pint at the pub.