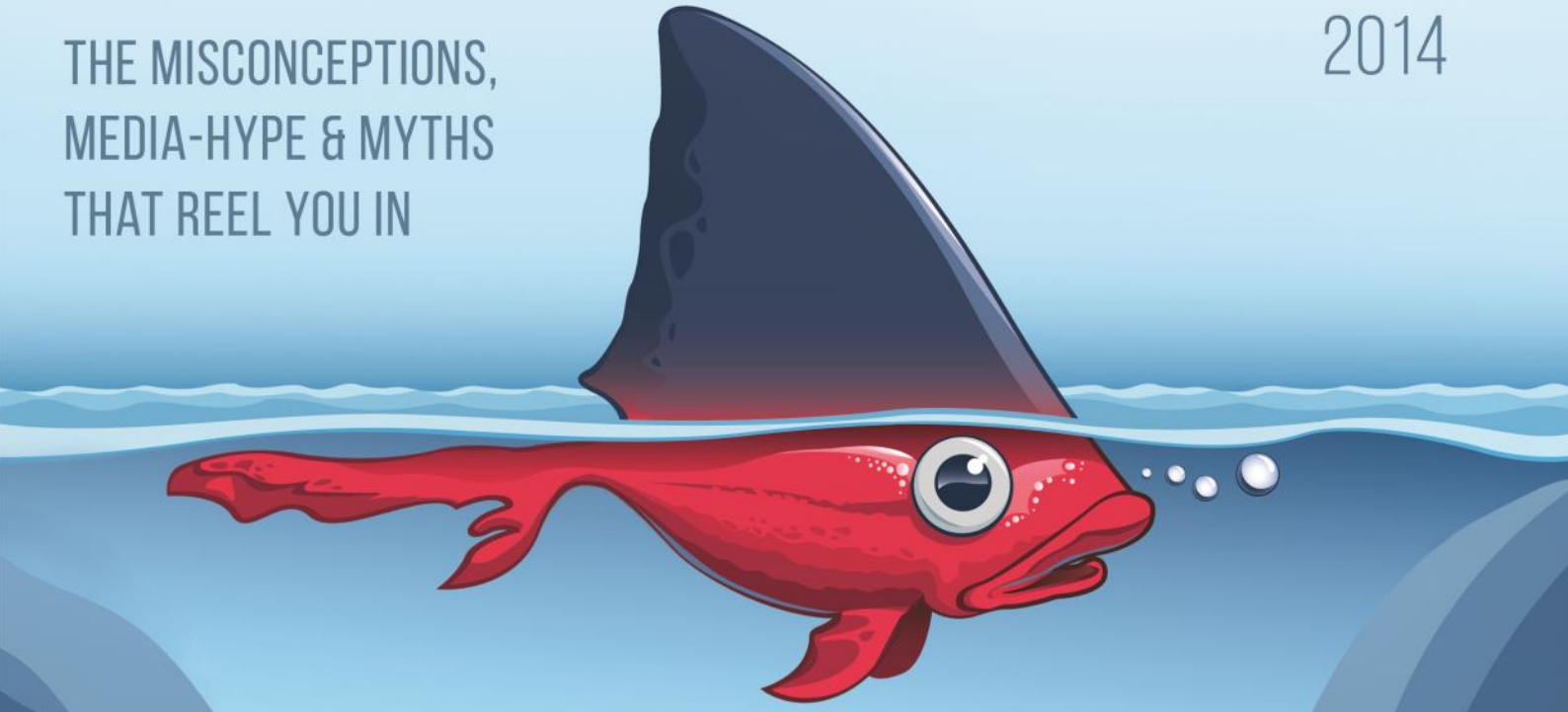
SECURITY+

MYTH VS REALITY

2014

THE MISCONCEPTIONS,
MEDIA-HYPE & MYTHS
THAT REEL YOU IN



APTs
802.11AC
EMAIL MANAGEMENT
GUEST WI-FI
CYBER INSURANCE

securityplusonline.co.uk

e92plus

WELCOME TO THE LATEST EDITION OF SECURITY+ FROM E92PLUS

Essential industry insights, opinions and interviews.

This month we are focusing on Myth v Reality: challenging the FUD, misconceptions and hype in the IT industry. The rate of new technology becoming available is matched by the increasing threat landscape, and it's hard to know where resources need to be focused.

How can businesses of all sizes protect against APTs? What does upgrading to 802.11ac wireless really bring to an organisation? How can you really keep your data protected? We take a look at these big questions.

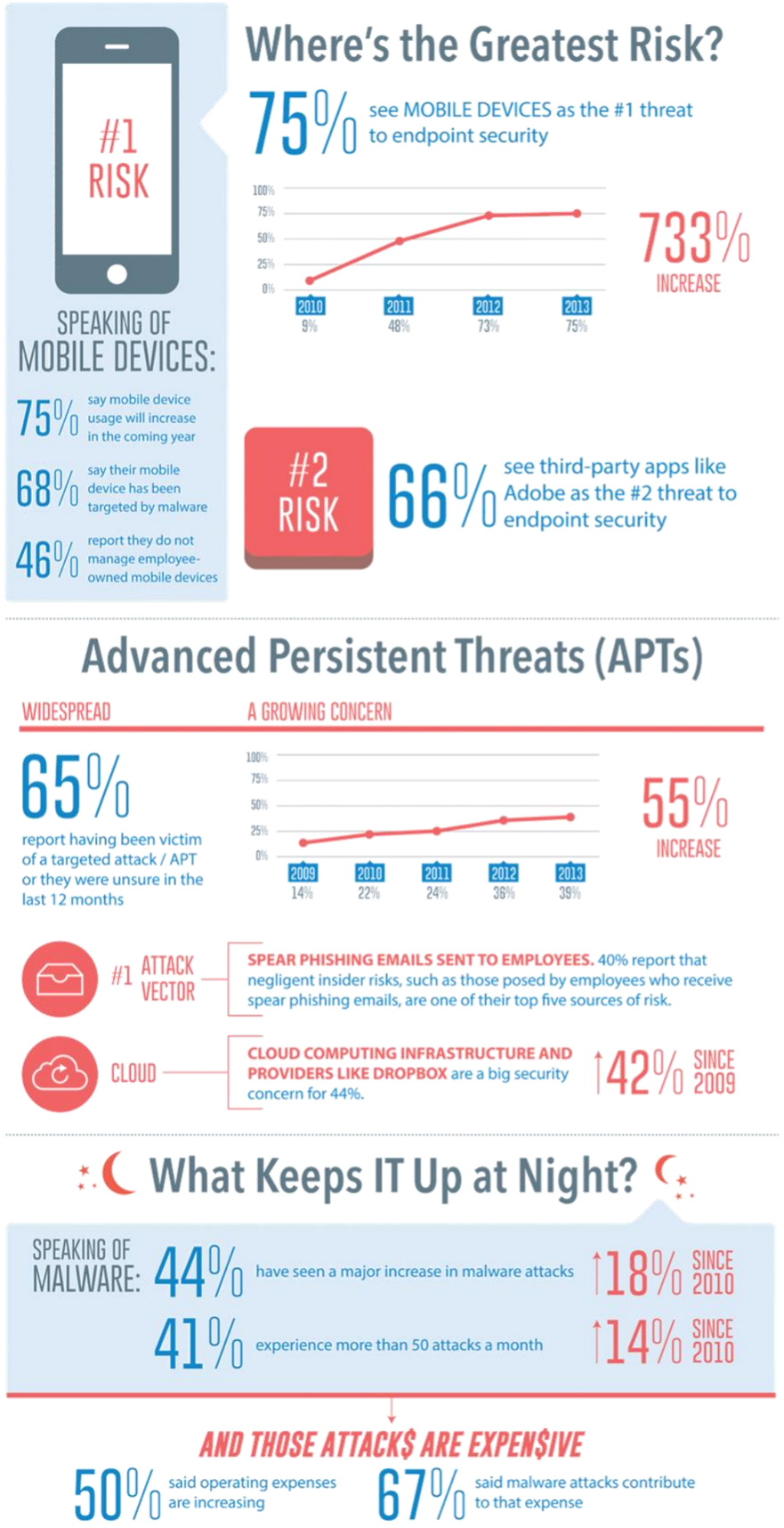
We also preview Infosecurity Europe 2014, the biggest event in the IT security calendar, and we'd be delighted to see you there.

Finally, we always appreciate feedback on Security+ magazine – so feel free to drop us a line at **securityplus@e92plus.com**. We look forward to hearing from you.

Mukesh Gupta
Managing Director of e92plus

20th ANNIVERSARY
CRN THE CHANNEL AWARDS 2013 WINNER

INSIDE THIS EDITION



WHEN APTS ATTACK

40% OF ORGANISATIONS HAVE BEEN ATTACKED IN THE LAST 12 MONTHS. IT IS TIME TO DEFEND IN DEPTH.

Pat Clawson is chairman and CEO at Lumension Security, a global leader in endpoint management and security. He may be reached at pat.clawson@lumension.com

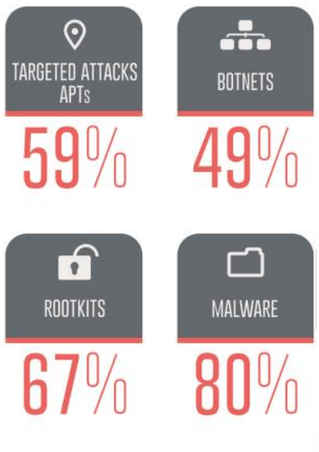
Countless organisations have fallen prey to cyber attacks - from high profile retailers to enterprises and government agencies. Some attacks have been high profile, for example the December 2013 data breach at Target, the third largest retailer in the U.S. that compromised tens of millions of customer accounts. Others went under the radar, lacking the fantastic numbers to merit a full-scale media exposé but damaging nonetheless.

Like enterprises, government agencies around the globe are of course at risk for this sort of attack and exposure too – some would argue they are targeted more frequently. In 2013, the U.S. Department of Energy (DOE) was attacked through an unpatched server and the personal information of its employees was compromised.

In 2014 we will certainly see more of these stories. The unfortunate reality is the cybersecurity landscape is not the same as it once was. No longer are we protecting against a piece of malicious code – we are defending against persistent adversaries. Every company, large or small, and every government agency has information that could be of value to a hacker – and if they decide to go after it, chances are good they will find a way to get it.

This is an attack method known as "advanced persistent threats," or APTs, which strategically target those in possession of valuable data or access to that data, and relentlessly attempt to steal it. The attacks tend to be professionally organised, sometimes by nation-states, and are highly focused on gaining complete control of networks in order to access the data they are interested in. Though every targeted attack is different, they do tend to follow predictable patterns, which is crucial for your defence.

WHAT ELSE KEEPS IT UP AT NIGHT?



Predictable Pattern of APTs

First is the discovery portion of the attack. If it were a traditional robbery, you might call this "casing the joint." It might be in the form of a targeted phishing email or a widely broadcast piece of spam – or even striking up conversations with government employees via social media. The idea is to get a picture of the defences the target is employing and gain access to the system.

Next, the adversary moves to stage two: distribute. In this step, the payload is delivered. This payload is typically custom-made for the particular government agency it's targeting, and is designed to be stealthy, stable and at times, sophisticated. The easiest distribution method is through third party applications, like Adobe or Flash, as vulnerabilities in those third party applications are so often left unpatched. They also might be delivered via malicious USBs, if the attacker has physical access, via SQL injection, or any number of other methods.

In stage three, the payload is exploited, or triggered, within the system so that the malware can execute. In some cases, the malware will be self-executing – for example, from a malicious webpage. Other times, it might require a user to open an attachment or malicious link. Often times, attackers will scale their attack, starting at easy-to-exploit (and easy to fix!) vulnerabilities, and scaling up to less common, harder to execute vulnerabilities until they find an opening that gives them the access and control they're looking for.

After access and control of a machine has been gained, the attacker moves on to stage four, where they escalate the attack to additional machines, often with lateral moves, across the network and gain complete control of the system. The payload will connect back to the attacker, often piggybacking legitimate or trusted communications, and will verify that the desired degree of control has been reached without detection.

With control of the system, the attacker will begin to execute their larger mission. Whether they set out to steal data or use the system to leapfrog to a secondary system, such as that of your partner, client, customer or even another government agency, the attacker will now be able to achieve their original end goal without interference.

By the time the attack reaches this final stage, it could have been going on for hours, days or even months. The exact attack payloads, the timeline and the goals change with every attacker and every attack. Yet the attackers who execute an APT methodology are persistent – hence the name – and if they can get in, they will.

Employ a Targeted Defence

The persistent nature of these adversaries is discouraging to say the least. But that doesn't mean the cause is hopeless. There are a number of steps that government agencies and companies alike can take to reduce risk and minimize the chances that an attacker can be successful.

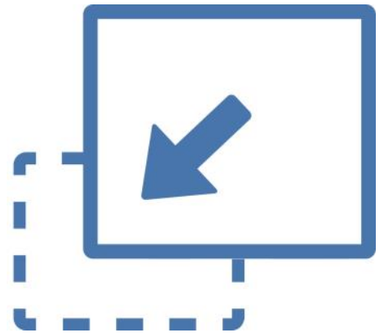
First, and foremost, is user education. Your users must know their role in the process and how to recognise common attack methods, including spear phishing, malicious links and malware-infested websites. Make sure that they understand what actions to take if they suspect their machine may have been compromised or they have been the target of such an attack.

Second, work to reduce your exploitable surface area. This starts with patching – particularly third party applications. Ensure your endpoints are managed and secured, preferably with multiple security technologies such as anti-malware, firewalls, anti-phishing and others. And, make sure you are running the latest versions of software and operating systems. You could also employ application whitelisting to ensure that only known, safe applications are allowed to execute on the machine.

Finally, watch for attacks. If you're not looking for it, an attack can easily masquerade as legitimate activity. But a watchful IT department can catch suspicious activity before it has a chance to do significant damage. Monitor assets and ensure that activities are logged and analysed. Watch to ensure users are not added to groups where they do not belong, and look for large or unusual data transfers.

Targeted threats are common, but it's surprising how effective basic steps can be at preventing them from affecting your agency. While it's easy to claim that time and budget constraints will limit defence capabilities and practices, the time and budget necessary to clean up after a successful attack is far greater.

EDUCATE USERS



REDUCE EXPLOITABLE SURFACE AREA

DETECTION & RESPONSE CAPABILITIES

ALWAYS BE THINKING DEFENCE IN DEPTH

Lumension
IT Secured. Success Optimized.

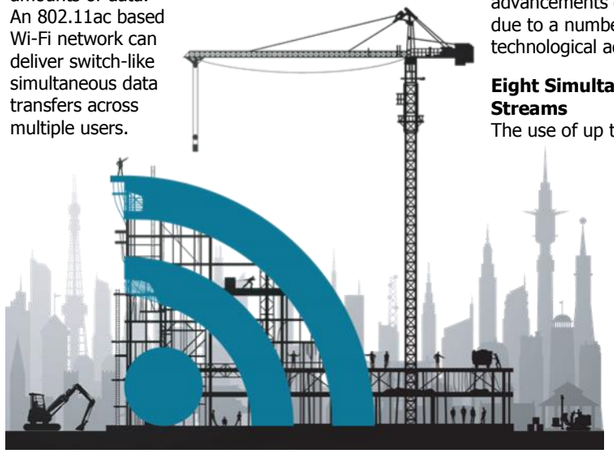
Lumension can help you combat APTs and defend in depth. Visit www.e92plus.com/Lumension for a free evaluation

BUILDING FASTER WIRELESS

BUT WHAT DOES 802.11AC REALLY DELIVER?

Millions of new wireless devices are activated every day and it's no wonder - the average wireless user has 2.8 devices. The volume of application data used by these devices will overtake the total traffic on wired networks by 2014. Video traffic will account for the majority of this increase, expected to be up to 70% of global traffic sometime during 2015.

Modern enterprises depend on anytime, anywhere access to communications, cloud services, and business applications including ERP, CRM, business analytics, video conferencing, and collaboration. The trend from desktop and laptops to tablets and smartphones, coupled with corporate acceptance of bring-your-own-device (BYOD) policies are changing the landscape. Wi-Fi networks must supply both higher performance and higher bandwidth. 802.11ac will enable new applications that were previously impractical with Wi-Fi connections, including real-time access to business information and ability to transfer larger amounts of data.



An 802.11ac based Wi-Fi network can deliver switch-like simultaneous data transfers across multiple users.

Mobile users can experience application performance similar to that of the wired network. Enterprises can deploy high bandwidth applications like video and collaborative tools to BYOD users.

Xirrus delivers the first 802.11ac AP of its class in the industry that supports 802.11ac on every radio. The XR-600 is a software upgradeable, low cost, cloud provisioned and manageable Access Point with uncompromised performance for low to medium density uses. The XR-600 supports Xirrus ACExpress™, which delivers optimized 802.11ac performance by ensuring faster 11ac clients operate on their own radio when possible.

In the real world, how does 802.11ac benefit your business?

The speed, range, and performance advancements of 802.11ac are due to a number of significant technological advancements.

Eight Simultaneous Data Streams
The use of up to eight simultaneous data streams from eight antennas is a key element of 802.11ac, allowing up to 6.93Gbps of throughput. This allows signals to be transmitted from and received by multiple antennas, increasing the data rate between endpoints. This doubles the earlier 802.11n standard of four streams which were able to transmit up to 600Mbps. However enabling 8 antennas on a single mobile device needs further technology advances. The currently available Wave 1 products support up to 3 data streams and the initial round of Wave 2 products are expected to support up to 4 streams.

Multi-user Multiple-Input-Multiple-Output (MU-MIMO)
802.11ac also introduces the concept of parallel transport through MU-MIMO, where multiple clients receive packets concurrently from a single AP. This allows an AP to transmit data to multiple client devices in the same frequency spectrum at the same time, increasing overall wireless system performance.

With 802.11n, whenever the AP transmitted data, all of the traffic at any instance of time was directed to a single client. As a consequence, if a set of devices included a mix of fast and slow clients, the fast traffic was often substantially delayed by the transmission to slower clients. 802.11ac MU-MIMO works by directing some of the spatial streams to one client and other spatial streams to other clients, at up to four at a time. MU-MIMO is especially effective where there are a large number of clients, for example, in stadiums, near hotspots, and in large enterprises.

Higher Precision and Sensitivity

In order to increase the transport rate, 802.11ac makes use of a higher rate modulation scheme known as 256-QAM, which transmits 33% more data than the 64-QAM used in the 802.11n standard. The signal level that receivers must distinguish is significantly smaller, requiring more sensitive receivers and higher precision transmitters. 802.11ac still supports lower QAM levels, which are used for extended range transmission and areas of client congestion.

80 and 160MHz Channel Widths
802.11n used a basic channel width of 20MHz with the ability to bond two channels into a 40MHz channel. 802.11ac uses 80MHz and 160MHz bandwidths while still supporting 20 and 40MHz channels. Bonding of two 40MHz channels to 80MHz results in a 117% increase in data rate over 40MHz, while bonding of two 80MHz channels results in a 333% gain over a single 40MHz channel. Wave 1 802.11ac products will support 20, 40, and 80MHz channels 802.11ac operates exclusively in the 5GHz frequency range. This avoids the congested 2.4GHz range that can experience interference from microwave ovens, Bluetooth headsets and other devices.

Beam Forming
Beam forming is a technique that optimises communications between APs and clients to counter interference. In beam forming, the AP communicates with clients to determine the types of impairment that exist between them. The AP then "pre-codes" the transmitted frame with the inverse of impairment such that when the next frame is received with better signal integrity. Since no two clients are in the same location and may move, beam forming must be applied on a client-by-client basis and constantly.

802.11ac is an excellent evolutionary step in Wi-Fi technology with new, significant technology. There are some challenges, however, in getting the most from the technology. Careful planning that includes anticipated usage over the next five years must precede deployments. APs that have the capacity, expandability, and control to handle the integration and migration to 802.11ac must be selected.

So where are you likely to look at deploying 802.11ac?

The higher bandwidth and MU-MIMO capabilities inherent in 802.11ac will allow business applications that were previously impractical over Wi-Fi, such as:

Large data transfers. Previously it was impractical to replicate big data volumes to portable devices and keep it in sync.

Wireless displays. Tablets will soon be every bit as capable as laptops, but lack screen area. As they become the platform of choice for businesses, the ability to link wirelessly to wireless-capable LCD displays and projectors will become possible.

Real-time updates. A wide range of time -critical applications, including ERP, CRM, and business analytics will be empowered by 802.11ac 5GHz availability.

Video conferencing. Reliable, distortion free one-on-one and multi-party video conference will become the standard with 802.11ac without special equipment.

Collaboration. Cooperative, real-time work on data files and documents, for business analysis and planning.

Key considerations for the next step

The theoretical data rates described are just that, theoretical. For 802.11ac deployments, and in fact for all Wi-Fi deployments, IT managers and users must be made aware of factors that affect real-world performance. The following are some important considerations in the deployment of Wi-Fi networks that include 802.11ac:

Wireless networks are not wired networks. Wired network users who share a Gigabit network can expect to see maximum performance, but wireless users are sharing bandwidth from any AP.

Migration to 802.11ac will take time—new devices come out gradually, and older laptops and tablets will remain in use.

Infrastructure must be upgraded as well. The bandwidth required out of 802.11ac APs will certainly exceed 1Gbps and may reach 10Gbps, so the core network (firewall, switches, etc.) need to be scalable.

More power. Multi-antenna APs handling 802.11ac speeds will likely require more power, so your switches need to be able to cope.

A new site survey may be needed. Wireless networks established as recently as a few years ago were probably designed for coverage and not capacity, so need to be reviewed.

It's all about the apps. With 802.11ac, a range of applications are now practical on mobile devices that were previously only used over wired networks or on laptops. Ensure you prioritise what's important.

XIRRUS FIRST PAST THE POST WITH THE JOCKEY CLUB

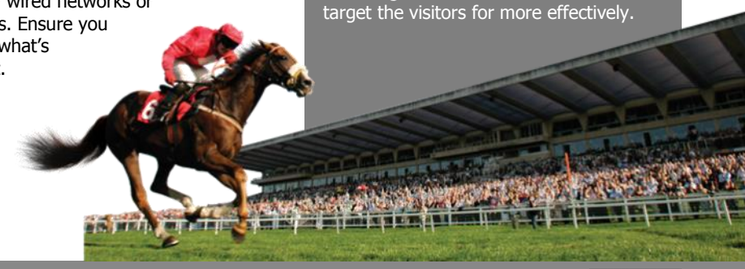
Xirrus delivered a bespoke, high performance Wi-Fi solution for this year's Cheltenham Festival (11th-14th March). Over 235,000 race goers attended the four day festival, benefiting from free wireless access with a simple sign-up process.

The new Wi-Fi network deployed at Cheltenham Racecourse is set to transform the way The Jockey Club can now use technology to more effectively engage with racegoers, members, staff, sponsors, media, business partners and even the jockeys themselves. The deployment equips Cheltenham Racecourse with proven technology to deliver high speed, reliable, wireless Internet access to thousands of mobile phone and tablet users in and around the venue.

The Xirrus-based wireless network will provide The Jockey Club with a number of dedicated wireless secure networks for guests, internal corporate users and sponsors. The solution is delivered on a fully managed Wi-Fi network that allows for growth and additional services to be provided to existing visitors and new customers.

Commenting on the launch of the Wi-Fi network at Cheltenham Racecourse, Ian Renton, Regional Director of the South West region of Jockey Club Racecourses, said: "Every year at Cheltenham we look to enhance the experience we offer our racegoers. Being able to provide free Wi-Fi is a fantastic innovation for our customers."

The Wi-Fi network will enable The Jockey Club to maximise fan engagement through providing an immersive experience to bandwidth-hungry visitors, generating new revenue streams and collecting customer data in order to target the visitors for more effectively.



XIRRUS

Xirrus are the leader in high performance, upgradable Wi-Fi. Visit www.e92plus.com/Xirrus for a free evaluation

THE FUTURE OF GUEST WI-FI

SMART. SEAMLESS. SECURE.

Delivering guest Wi-Fi is a key part of customer service for many organisations - yet when you need to deliver connectivity to up 20,000 users and need to cater for BYOD, the challenge is significant. Rather than simply adding more Access Points, a cohesive approach is needed with a solution that fully integrates Wi-Fi connectivity, security, guest access and administration.

What are the challenges that organisations face in delivering advanced guest Wi-Fi?

- Monolithic point solutions are complex to implement and manage.
- Solutions have to integrate with existing infrastructure and easily scale with demand.
- Need simple tools to gain in-depth visibility and enforce granular control.

What are the key requirements in choosing a new solution?

- Mitigate business risk and provide secure connectivity to employees, partners and guests. Providing guest Wi-Fi brings a number of security requirements to protect customers and your own network
- Provide a wired-like experience: user expectations are high, especially for laptop users who demand the same performance they had with Ethernet
- Reduce cost of the operating solution and be able to scale as the demand grows. Flexibility isn't just adding APs - the deployment needs the bandwidth and capacity at every point, as well as allowing for new technologies (such as 802.11ac)
- Deliver robust infrastructure to enable business and monetisation services. Everyone wants ROI on IT investment, and guest Wi-Fi is almost uniquely placed to deliver fantastic returns from simple payment gateways to social media interaction and new levels of personalised customer engagement

Of course, different industries have specific requirements - here are examples of typical industry specific scenarios:

Enterprise
Tiered access for employee BYOD, partners and guests.
Secure BYOD access for employees.

Education
Enable students to bring their own devices.
Facilitate faculty/teacher/student access to digital learning.

Stadiums and Arenas
Enhance fan experience with tiered access and seamless roaming.
Drive new services and marketing initiatives to monetise fan presence.

Retail
Provide guest access to shoppers and monetise in-store visits.
Drive marketing initiatives to build and execute loyalty programs.

Convention/Exhibition Centres
Delivered tiered services to convention attendees with billing integration.
Allow seamless roaming for vendors and attendees.

Service Providers
Provide guest services & Wi-Fi offloading.
Integrate with 3rd party billing services to provide tiered services.

A complete solution needs to be highly secure with industry standards based encryption, access control integrated with Active Directory credentials, URL filtering and highly controlled access for guest and BYOD users. It's important to scale quickly and easily (especially handling varying numbers of concurrent users, such as for sporting or exhibition events) while being robust across a large physical environment and distributed architecture, possibly with open public spaces.

New technologies are making these steps easier. Having centralised controllers is no longer required, with intelligence at the edge reducing the added cost of controllers and increasing flexibility - and significantly reducing unnecessary network traffic when applying policies, managing applications or content controls.

A new approach from Xirrus and Ucopia Communications.

Xirrus and Ucopia have partnered to provide a fully integrated solution to meet these challenges, and enable organisations to embrace the opportunity that BYOD and guest Wi-Fi brings.

Their partnership significantly reduces the TCO and IT operational overhead by automating provisioning, policy definition and enforcement from the cloud, reduced number of APs, fewer cable runs and switch ports while providing higher density coverage.

The solution delivers highly customisable web infrastructure and multi-portal capability integrated with online payment and billing services to deliver a comprehensive solution for business and monetisation services.

How the solution works.

The integrated solution is tested and proven in customer environments and gives you the flexibility to implement in the cloud or on-premise. It includes full integration with the domain infrastructure (such as AD or LDAP) for network users, yet for simple wireless management it can run from the cloud with plug and play Arrays and APs. Application Control provides granular priority control over traffic. Guest access can include advanced billing options or extensive social media, marketing and sponsorship integration. Above all, it's scalable and designed to grow with technological updates and increased usage - providing the best ROI.

For a free evaluation or more information, contact us today.

"In September 2012, we decided to increase the personalisation of education by providing an iPad to each of our students and teachers. With this tool, we wanted everyone to be able to create, access, and especially share information quickly and easily".

Requirements

To support this project, we needed a very efficient and secure Wi-Fi network. The first challenge was to manage the concentration of a large number of users in a small space (about twenty students per classroom) and ensure their mobility through the campus without any loss of connection. In terms of security, it was extremely important for us to know and decide who can connect to the network, at what time of the day, while filtering content. In addition, we needed a fast and fluid network, capable of holding the connection load at all times." Matthew Goblet, IT Manager, BSP

The Implemented Solution

Thirty Xirrus Wi-Fi stations were deployed. Each station has up to 8 radio antennas, which can connect up to 400 active users — this is 4 to 8 times more efficient than the competitive products. The Wi-Fi school network has been sized to provide a high broadband connection to 1,000 iPads simultaneously. These high performances limit the number of equipment, simplify deployments and allow the installation of antennas in the hallways, not in the classrooms.

This choice of architecture allows you to associate performance and reliability while optimising investment capital and operating costs. Two redundant Ucopia authentication servers manage network access according to the profile of each user (students, teachers, administrative staff or visitors), and then assign specific permissions: bandwidth and connection time, permitted applications and content.

The Internet access for students is filtered to avoid connections to inappropriate websites or with no educational value.

Moreover, the Ucopia solution integrates very simply with the existing network architecture, and in the case of the British School of Paris, Ucopia authenticates students directly from the school directory to give access to the Internet and other services.

This architecture greatly facilitates managing the network: indeed, when a student is declared in the school directory, they can access the Internet using the login and password defined in this directory.

The Results

The assessment made by students is very positive. If there was a little hesitation at first and some felt the need to be guided, they quickly realised the benefits that the tablets and Wi-Fi network bring. Wherever they are in school, students can instantly search for the latest Internet resources and access them. They no longer need to carry their books and notebooks as much, because they are just a click away from their teachers, their class notes and homework.

In the end, they realise that it helps them prepare for the future by taking advantage of the best technology. Some even wonder how they worked before!

The overall cost of the Wi-Fi network is less than 150 euros per user, and was partially covered by the savings of prints (cut in half) and the digitisation of some textbooks.

UCOPIA COMMUNICATIONS

Ucopia Communications can help you enjoy amazing ROI on your Wi-Fi. Visit www.e92plus.com/Ucopia for a free evaluation

SECURE THE CLOUD... IN THE CLOUD!

Taking trust-in-the-cloud to a higher strata, SafeNet's cloud-delivered authentication offering, SafeNet Authentication Service, has been granted the ISO 27001:2005 Certification, thereby achieving the highest attainable credibility ranking for information security management.

This is exciting news for SafeNet and its cloud authentication offering as ISO 27001:2005 is an internationally recognised security standard. This inspires confidence in IT and infosec professionals seeking to move resources to the cloud without compromising security.

As noted in SafeNet's recent report based on a global survey on data centre consolidation, 74% of IT and security professionals see compliance and data protection as core must-haves when sourcing cloud solutions.

"The adoption of new technologies – such as big data, mobility and cloud-based services – has pushed data centre consolidation to the top of the priority list for many businesses. Yet it is clear that security concerns combined with a lack of resources are hampering the progress of such transformations," said Prakash Panjwani, Senior VP and General Manager of SafeNet, with respect to the survey. The ISO 27001 certification brings trust to the cloud computing equation, allowing cloud computing efficiencies and convenience without sacrificing data integrity and protection.

ISO 27001 was established by the International Standards Organisation for ensuring the confidentiality, integrity and availability of information assets owned by an organisation. Central to its implementation is the identification of information assets, potential threats and risks to those assets, and the implementation of appropriate controls to reduce asset-related risks.

The value of accreditations such as the ISO 27001 standard lies in the fact that they are granted by independent third party audit companies, pursuant to in-depth audits conducted on premises at the applying organisation. These types of assessments provide transparency and accountability, and ensure that SafeNet is implementing globally-recognised best practice measures to guarantee that it offers the best quality products and services. In SafeNet's case, leading certification firm UL-DQS Inc. performed the audit, visiting the sites in Ottawa and Belcamp to assess their adherence to the ISO 27001 standard.

The ISO 27001 certification is just one facet of SafeNet's broader Next Generation Authentication offering, whose cornerstones include a Trusted Authentication Environment based on industry-recognised standards, as well as ensuring that our products and services meet globally recognised security standards such as FIPS, Common Criteria, and now also ISO 27001:2005.

"SafeNet offers a viable cloud service alternative to the traditional platform approach for identity management. The SafeNet Authentication Service provides secure, automated authentication-as-a-service and web SSO without the infrastructure, support, and cost overheads of the traditional identity management model," said Andrew Kellett, principal analyst, IT security solutions, Ovum.

For your free evaluation of SafeNet's market leading authentication for remote access, virtual desktops or cloud applications, contact us today.

REMOTE ACCESS

With a mobile workforce and flexible working practices, remote access becomes more of a threat - and user authentication is an essential first step.

COLLABORATION PORTALS

As they open their applications to partners, vendors, and customers via Web portals, organisations all need authentication - providing essential security for confidential data and documents wherever they are hosted.

VIRTUAL DESKTOPS

VDI is finally breaking through, helping reduce complexity, lower costs, and improve flexibility for users. With data held on infrastructure rather than devices, it's access anywhere - and so access must be authenticated.

CLOUD

More organisations are moving to the cloud, but the multi-tenant cloud model—where several customers' applications may be handled by one server—means that securing user access is a much more significant issue.

MYTH

CLOUD AUTHENTICATION IS NOT SECURE

BUSTED

SafeNet Authentication Service has been granted the ISO 27001:2005 Certification, thereby achieving the highest attainable credibility ranking for information security management .

MYTH

AUTHENTICATION IS JUST FOR REMOTE WORKING USING VPN CONNECTIONS

BUSTED

Corporate applications are no longer just on the network, they're in the cloud too. Users connect on corporate devices - and with personal ones as well. This means that access to critical data needs to be authenticated for every platform, for every device.

MYTH

SOME SMS AUTHENTICATION VENDORS BELIEVE THEY PROVIDE THE SIMPLEST STRONG AUTHENTICATION.

BUSTED

Most SMS authentication providers do not issue a PIN that means it's not two-factor authentication. SafeNet automates the provisioning, administering and managing of users and tokens which reduces the single biggest cost of an authentication system, often by an order of magnitude.

MYTH

SOME AUTHENTICATION VENDORS CLAIM THEY ARE THE PREFERRED CHOICE FOR REMOTE ACCESS VENDORS.

BUSTED

Remote access vendors do not exclusively partner with one authentication vendor. SafeNet has technology partnerships with many complimentary vendors, including; Citrix, Microsoft etc. SafeNet protects everything - from traditional network applications such as VPNs to cloud and SAAS based applications

SafeNet

See the reality behind the myth with SafeNet. Visit www.e92plus.com/SafeNet for your free 2FA Tokens

FROM "FUD" TO FACTS

DEALING WITH MODERN THREATS

Understanding exactly what an Advanced Persistent Threat (APT) is can be difficult as different interpretations are being used. Marketing hype and FUD (fear, uncertainty and doubt) have clouded the facts about a very real danger to organisations of all sizes.

While the news media use stories of APTs to generate buzz, tools and techniques used as part of an APT are real weapons in data thieves' attack arsenals.

The term 'Advanced Persistent Threat' was first coined by the US Air Force, circa 2006, to describe complex (i.e., 'advanced') cyber attacks against specific targets over long periods of time (i.e. "persistent'). From 2006 through 2009, APT knowledge was really limited to military and intelligence services throughout the world as attacks were really focused on these sectors. That all changed in December 2009 with the Google Aurora attack.

This single event transformed the term 'APT' from a cryptic military abbreviation to a topic worthy of the mainstream media. Similar attacks carried out by cyber-criminals stealing data from businesses for profit are also generally addressed as APTs by security vendors and media. We have seen attackers go after customer records, blueprints, product roadmaps, source code, and other confidential information. Large corporate and government organisations with a treasure chest of intellectual property (like source codes) are high-value targets for cybercrime. Criminals using APTs want data, so the more valuable an organisation's data, the more likely it is to be targeted.

A key difference between most malware and an APT is it's ability to persist – that is, to evade detection by network security controls while still collecting and extracting data. In many cases, developers use unknown zero-day exploits so there are no antivirus signatures available to provide protection. Here, cybercriminals constantly refine their attack methods to breach organisations and steal critical data. Unlike the majority of malware, which randomly infects any computer vulnerable to a given exploit, APTs target specific organisations with the purpose of stealing specific data or causing specific damage. Stuxnet is a great example of this attack method and is a text book case of an APT. The Worm was discovered July 2010 and is the first specialised complex malware to only target industrial software. It was aimed at compromising the Iranian nuclear program and is believed to be from a well-funded group of 5-10 people over 6 months.

APTs exploit the full spectrum of attack methods, including email phishing, website malware, Trojans, and more by following the staged-attack model to bypass traditional defences. They do it through reconnaissance, luring victims, redirecting web traffic, executing exploit kits, deploying dropper files, calling home and ultimately stealing critical data. Since each of these actions could occur on a different part of a network, or over a different communication channel, cybercriminals can break in and steal data at will. The ingenious methods used in the past show the in-depth knowledge of the attack developers. This requires enormous amounts of research, and the entire process may take months or even years. The perpetrators are willing to invest time and money into achieving specific objectives. Attacks of this nature become more frequent, with social engineering techniques being adopted by a broader base of attackers for ongoing attempts at purloining data. Information available about individuals and their habits in the public domain often comes in handy to attackers. Some of the most prominent examples of APTs include Stuxnet, Aurora, Flame, Nitro, Night Dragon and Duqu.

Whether creating a new security strategy, assessing or improving the company's existing security program, or even under attack, today's CISO has the difficult task of balancing the security books and accommodating the economic needs of the business in complete alignment with the mission of maintaining the operational lights in secure working order. Each year, apart from the APTs, CISOs must deal with the business-as-usual security issues. The biggest challenge CISO's face is 'Where to begin first?' as every aspect of a business is important. Organisations are vulnerable to targeted attacks and advanced persistent threats if they rely on security solutions that only address part of the advanced threat kill chain. Defending against advanced targeted attacks requires a new approach with enhancements that include advanced threat protection with expanded inline sandboxing, malware isolation to heighten data loss prevention, end-user phishing education and new platform support.

<12HRS

IS ALL IT TAKES FOR CRIMINALS TO EXPLOIT DISASTERS

20%

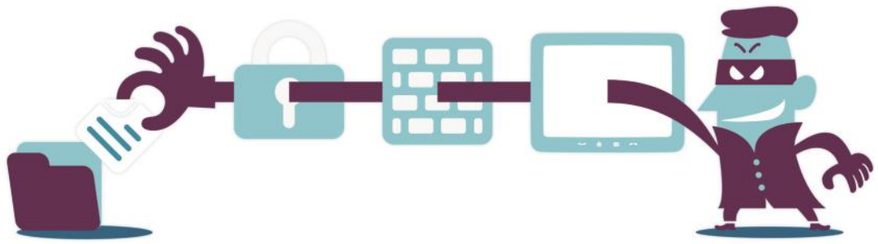
OF EMAILS SENT WERE SAFE OR LEGITIMATE

85%

OF MALICIOUS SITES WERE FOUND ON LEGITIMATE WEBHOSTS

>50%

OF CORPORATE EMAILS ARE SENT OUTSIDE OF TRADITIONAL NETWORK DEFENCES



While APTs don't target everyone, everyone should understand how APTs work — because these same techniques are now being used by cybercriminals in targeted attacks designed to steal sensitive data from all kinds of organisations. APTs are also a prototype for other targeted attacks that are now victimising businesses of all shapes and sizes. For example, the same APT technology used by China to hack Google, Adobe, and approximately 30 other companies in the Aurora Internet Explorer zero-day attack is now being used by cybercriminals to steal data from other organisations as well. Stuxnet, which infected Iran's uranium enrichment centrifuges, can be a source of inspiration for cybercriminals targeting enterprises.

Though the term originally referred to nation-states engaging in cyber espionage, APT techniques are also being used by cybercriminals to steal data from businesses for financial gain. Although victims of an APT attack typically belong to a handful of industries, organisations which might not be the specific target might be one piece of the attackers' puzzle because of information that is deemed valuable to them. It is better for these organisations to be cautious rather than be naive and think that they are unlikely to be targeted. Since most APTs use custom-developed code and/or target zero-day vulnerabilities, no single IPS or antivirus signature is likely to positively identify the threat.

There is no such thing as an all-in-one solution to APT attacks. Because different attack vectors are used, a multi-layered approach to preventing (or at least minimising the impact of an APT) is required. By shifting the paradigm from prevention to detection, organisations can take focused, intelligent action to stay safe.

Neil Thacker is Security Strategist at Websense, you can follow him @nt_hacker

WORK SMARTER, NOT HARDER:

CHALLENGING MYTHS WITH INDEPENDENT SECURITY TESTS

We've all been there. Your boss, or their boss, asks if you have the most advanced IT security solutions in place. You have spent months, or years, developing a security strategy that protects your organisation from data theft and keeps your business ahead of the competition.

Miercom has conducted an independent third-party validation of:

- Websense TRITON Web Security Gateway Anywhere
- Blue Coat ProxySG 900-20 Secure Web Gateway
- Check Point 12200 Appliance Next-Generation Threat Protection
- McAfee WG-5500-B Web Gateway
- Palo Alto Networks™ PA-2020 Next -Generation Firewall

Miercom independently sourced a URL sample set unknown to any of the vendors. Two types of tests were conducted to evaluate the ability of the appliances to block threats and malicious content.

Test results show that Websense TRITON outperformed all competitors by demonstrating superior web security effectiveness against both known and unknown advanced threats, in several key attack areas including identification of exploit kits, redirects, and drive-by downloads.

Using independent tests, like this Miercom assessment, is a way to work smarter—not harder and see the reality behind the marketing hype and myths.

You can download a copy of the full report from **www.websense.com/miercom2014**

websense

Websense stops more threats. Visit www.e92plus.com/Websense and we'll prove it

Anti-Virus has been a central component of network and endpoint security for many years, and it's a central part of many IT budgets. But is it fit to defend against modern threats? With the network no longer a controlled, secure perimeter, can traditional endpoint technologies protect against targeted, aggressive malware that no longer fits established patterns? Or do we need a new approach?

We spoke to Melih Abdulhayoğlu, the CEO of Comodo Group who he founded in 1998. He also works with The Scientific and Technological Research Council of Turkey, also initiated the Common Computing Security Standards Forum (CCSS), a voluntary organisation of security software vendors, operating system providers, and Internet browser software creators who are working together to mitigate the risk of malware and protect consumers worldwide

How can conventional antivirus scanners deal with a tidal wave of new malware each day?

The short answer is - they can't. Independent tester AV-Test Labs recently estimated that there are up to 55,000 new malware variants released into the wild each day. Other security firms claim that they identify as many as 200,000 new threats per day! Comodo's own network reports up to 300,000 malware variants every day. This makes it virtually impossible for the files of known viruses used by conventional scanners to be fully up to date.

To make matters worse, hackers are increasingly using the strategies developed originally by governments for espionage known as "Advanced Persistent Threats". APT's by nature are similar to conventional attacks but are generally harder to detect and prevent because they use unknown zero-day exploits that have not yet been identified for inclusion in virus scanners or addressed in security patches.

Scanning systems have been around a while now. Why do you think they are still flawed?

The first antivirus software was created in 1987 to clean an existing infection. Remarkably, this is the approach used by most scanners to this day! You only remove infections that have already occurred. This is like focusing on stain removal, as opposed to stain prevention. If we examine this logically, this standard approach is fundamentally flawed. The scanner compares each file run to a signature file of known viruses, a so called "blacklist". There are really only three possibilities:

- The file is Good: If the file is not infected you are ok, of course.
- The file is Bad: If the file has a known infection, it gets cleaned and you are still ok
- The file is Unknown: If the file has an unknown infection it does not get cleaned and your computer can be compromised.

Clearly, relying on what we already know creates a huge gap that hackers can exploit. Security experts have understood this for some time and have long advocated a "layered approach" to internet security. This means that the conventional approach of matching a file to a signature file, AKA a blacklist of known malware is just one layer of protection. For example, if a malware file gets past the blacklist it may still be identified as a threat using heuristic behaviour analysis. Regardless of what the blacklist says, if it acts like a threat it might just be a threat.

So you are saying that a multi-layer defence approach is the answer?

It's part of the answer. So far we are only discussing the detection of threats. Unfortunately, there is simply no perfect detection method.

Virus makers are smart and there is a lot of money in it. Why rob banks when you can sit in an apartment in Eastern Europe and operate a botnet that sends out malicious spam to control victims' computers? They will always come up with ways not to be detected. In their own nefarious way, they are very professional in their development efforts. They test their malware against the major scanners and their heuristics patterns before releasing them ensuring they will have success.

This is why the last layer of defence cannot be "detection"; it must be "containment". This means that if a file is not proven to be safe, it is not allowed access to a computers operating system and files. The principal vehicle for this is a concept called a "sandbox". A sandbox is an operating environment where a program file can run isolated from the rest of the computer system. If the program turns out to be malicious it will be unable to harm the system.

It's not surprising that there have been increasing uses of sandboxing technology in recent years. The standalone Sandboxie is popular among tech gurus because you can choose to run a program in a protected environment. Some major internet security systems provide a sandbox environment, but they also require detection and user interaction.

IS ANTI-VIRUS DEAD?

NO, BUT MALWARE DEFENCE NEEDS TO DEAL WITH THE REAL WORLD

Ask yourself this: Right now, how many files are sitting on your servers and endpoints that have unknown infections? You don't know?

Of course not! It is impossible to know the unknown. That's the very definition of unknown!

So how does Comodo implement a containment strategy with its systems?

Comodo takes a unique approach to sandboxing for both our enterprise and consumer protection systems. We call it "Default-Deny" with Auto Sandboxing. This is the only approach that can provide perfect protection because it is the only viable strategy for dealing with the unknown threats we discussed earlier.

Comodo's multi layered defence checks files against a "Whitelist" of known valid programs, compares files to a blacklist signature file and uses heuristics to identify threats. With Default-Deny, however, failing to identify a file as a threat is not enough. There could still be an unknown threat in an unknown program file. Default-Deny requires that a file be verified as safe to be run by the operating system.

That might sound too restrictive, but that is where Auto Sandboxing comes in. Unverified and suspicious files run safely in the Comodo sandbox where they can do no harm if they turn out to be malicious.

The security gap presented by unknown threats, and left open by other systems, is closed tight.

You seem to be very confident in your containment approach. Can you back it up?

There is no such thing as perfect detection. But with a sandbox containment approach, Comodo can provide perfect protection. That is why we provide the industry's only warranty protection that guarantees your computer and network will be virus free.

Our confidence in our systems and protection strategy is based on experience. You may have heard of the CryptoLocker virus, the ransomware program that hold computer users hostage by encrypting files and demanding payment to unlock them. Security experts have called CryptoLocker the perfect, unbeatable malware.

Unbeatable? Not to Comodo. With over 70 million total installations of Comodo Endpoint Security there has not been a single reported incident of CryptoLocker on a Comodo protected machine. **In fact, in over 6 years we have never had to pay a claim for our $5,000 virus free warranty protection for users of Comodo Endpoint Security!** That is why we call our protection "ironclad".

More than that, it aligns our interests with that of the computer user. Our competitors actually make money when their product fails, by charging to remove viruses that their systems failed to protect them against . That is plain wrong, and we provide a guarantee to demonstrate our commitment to a product that offers 100% protection, and does exactly what we say it does.

LAYERS OF ENDPOINT DEFENCE

Even with advanced sandbox protection, endpoints need layers of defence. Here are 5 key layers you need to stay secure:

Firewall: A highly configurable packet filtering firewall is the first line of defence

Sandbox Technology: If all malware viruses are automatically executed in a sandbox environment, nothing can infect your systems, even zero day attacks.

Host Intrusion Prevention: IPS monitors all application and activities, and blocks malicious activity and programs.

Blacklist/Whitelist Detection: Classification can quickly and easy automatically allow or block applications from running.

File Reputation Lookup: Authenticates every executable and auto-sandboxes unrecognised processes and applications.

WHY ARE TRADITIONAL AV APPROACHES OBSOLETE?

APT ATTACKS BYPASS SIGNATURE BASED ANTI-MALWARE SOLUTIONS

THESE ARE ZERO-DAY ATTACKS, UNKNOWN UNTIL THEY ARE RELEASED

THIS MEANS IT IS NOT DETECTED AND PROTECTED AGAINST BY LEGACY AV

IF YOU HAD AN UNKNOWN ILLNESS, WOULD WORLD PHARMACEUTICAL COMPANIES HAVE A READY MADE CURE?

NO.

COMODO

Enjoy proper protection - and $5,000 malware warranty. Visit www.e92plus.com/Comodo to try Comodo for free

IS THE OUTLOOK BLEAK FOR EMAIL MANAGEMENT?

We all agree that email is a fundamental part of our working lives, evolving from the mere sending and receiving of messages to what it is now: arguably our main method of accessing information day to day. The problem is, with the ever increasing quantity, what do you do with it all?

Some users opt to delete any emails they feel they no longer need, only to find themselves regretting that decision a short time later. Your IT department will tell you this isn't the solution to a full inbox, as they spend a large portion of their precious time searching through archives to retrieve it. In fact, in a recent survey we conducted, **80% of IT professionals confirmed that they regularly restore email from archive** on a regular basis.

So, what other options do we have when confronted with a full mailbox? Creating archive PSTs? This is a relatively quick fix and **creating multiple archive PSTs is the choice for 48% of those we surveyed** - yet this option solves one problem whilst inadvertently creating a more serious one. Securing sensitive data is a top priority for any organisation and this is made almost impossible when potentially damaging data is stored locally on mobile devices which, with their users, leave your network – and therefore your control.

More importantly, **95% of respondents confirmed that their users access email from a mobile device**, so it is highly probable that you will have to deal with this scenario at some stage , if you haven't already.

60%

of users regularly reach their mailbox limits.

43%

of organisations maybe be unable to defend a legal challenge because they don't retain email

48%

of users create local PST files to make room in their mailbox....but

8%

of IT Managers don't know if their users do this!

90%

of users send large attachments to internal distribution lists

7%

of IT Managers have refused to run HR or FoI searches due to lack of time or resources

Our survey also uncovered some rather worrying statistics regarding the length of time users keep emails. When you consider that all personnel email records should be kept for at least 6 years AFTER they cease to be employed, it is very concerning that **50% of organisations only keep emails live for a year**. Even more so that 37% only keep them live for 6 months! This results in another burden being placed on an already strained IT department, as they become bombarded with requests to restore deleted emails. Not being able to access the emails you need is inconvenient, annoying even, but when those emails contain details that are vital to an HR investigation, and you may face serious legal challenges – deleting those emails you "didn't need" suddenly becomes a lot more serious.

It seems to be common practice for IT staff to search for emails in relation to **HR investigations or the Freedom of Information act with 72% of people receiving such requests**, but what happens when they can't provide required information? It is a legal obligation to provide email records when requested and failure to do so can result in severe punishment. The fact is, we shouldn't be leaving such crucial matters to chance, in the hope that a human error won't result in a huge fine. Organisations constantly underestimate the importance of keeping email records.

If we take a quick look at some of the answers people gave as the biggest challenges to email management, you'll see some familiar pains:

- Misuse of email as a document storage medium
- Managing the sheer quantity
- Security
- Mailbox sizes
- Proliferation of PSTs

And of course...

- **People!**

Ah yes, people. To a certain extent, and with enough time spent on it, you could roll out email retention policies and keep a close eye to ensure compliance with the majority of the other answers given. However, can you guarantee a colleague won't get a little trigger happy with the delete key as they are confronted with that frustrating "mailbox full" error message? Organisations across the world implement technologies to help counteract human error to protect their network, whether it be a firewall, anti-virus or application control – so why wouldn't you do so for email?

Organisations can no longer ignore the importance of information security around email. Doing so can hurt the organisation's bottom line in terms of lost data, breaches of trust and loss of business partners. The value of the data your business processes can be measured in a variety of ways.

One way to approach the issue of information security is to view it through the lens of the **CIA Triad - Confidentiality, Integrity and Availability**.

The CIA Triad is an established, well known model for security policy development, used to identify problem areas and necessary solutions for information security.

Confidentiality, integrity, and availability are the core of this lens and a good place to start when building an information security system that protects what might be your businesses' most valuable assets.

Any searches that users carry out should be strictly controlled and monitored for everyone's security and protection.

Monitoring the integrity is key in determining if an information security system is effective. If email data is to be protected, then it must be protected in its original format. The ability to modify an email after it has been sent or received is not acceptable for maintaining information security.

Likewise, deleting emails is unacceptable if required to be kept by Law. Data integrity for archiving emails means the email is preserved exactly as it was sent or received.

The answer is a simple but efficient email management solution that automatically archives a copy of every email sent or received, both internally and externally, in real time. These identical copies form the archive, with every email digitally finger printed, time stamped, encrypted & compressed. The email is frozen in time & monitored.

Cryoserver's solution provides essential features to help keep data secure:

- User searches are strictly controlled and monitored, with full audit logs
- Searches can be carried out by Directors, HR or Security Teams without IT involvement
- Emails can't be modified or deleted after they've been sent or received
- All emails are finger printed, time stamped, encrypted & compressed
- Every email is frozen in time and fully monitored

Email archiving can also be an essential part of maximising the performance of the email server, without overloading it with large volumes of data that is rarely accessed.

With Microsoft Exchange 2003 support coming to an end, migration is another key project we can help with.

Contact us today for a free evaluation to see how Cryoserver can reduce the load on your email server and protect your users, company and data.

THE SECURITY+ GUIDE TO DOCUMENT RETENTION

Whatever business you are in, here are some important facts about email that you need to know:

- An **email can be edited in UNDER 5 seconds** using Microsoft Outlook. If you don't protect against this, you could leave your organisation exposed
- **All personnel records sent via email MUST be kept for at least 6 years** AFTER the employee ceases to be employed
- **Emails are legally binding contracts** and their contents can be admissible in court
- Any **access to a colleague's email should be audited** – noting which emails are viewed and why
- Any pension scheme rules must be kept for the duration of the scheme – **sometimes as long as 80 years**
- **All records relating to sickness and absence must be kept for 6 years** (including dates and causes of sick leave)

If you're unsure, Cryoserver can provide a free consultation to help ensure your organisation is compliant - contact us at **www.cryoserver.com/DidYouKnow**

REACHING FOR THE CLOUD

If we dare to share the fact we work in IT, many of us will regularly be faced with the question of "what is the cloud?". The answer will vary depending on audience, but often it's simply "data or applications that are located on someone else's computer".

Another favourite is "a data centre is Arizona", simply as that's as random as the reality of where our data really is!

The term "cloud" was popularised in general culture, thanks to Apple and their iCloud, to allow your Apple devices to be backed up into an offsite location. Terms such as cloud computing have been used by Google, Microsoft and Salesforce, who give application access without having to connect to servers within your organisation. We hear of terms such as Cloud Backup, where your data much like the Apple iCloud principle, is held in an offsite location, although that is again a more consumer focus. Amazon's cloud services such as AWS and Microsoft's Azure platform have also helped drive take up of cloud services, whether managed by individual companies or simply used as a easy platform by service providers. We even have private clouds, which stretch the definition - as that often just means on -premise!

So it's clear that the cloud is often a marketing term, rather than being a technological solution to all our IT challenges. It's simply the most recent incarnation of previous terms - in the not too distant past, there were terms like, Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), which described the solution being provided. Even further back, the term ASP (Application Service Provider) offered hosted/managed applications, but the

approach failed to reach the mainstream largely due to internet connectivity being too slow and limited demand from mobile workers and devices (unlike now).

The cloud is the current term of choice, and widely used. But in terms of a definition, what should it include?

- **Uptime**
  Delivered via multiple servers and multiple data centres, with the various failovers to ensure availability
- **Security**
  Meeting compliancy regulations, such as physical security, virtual security, encryption, firewalls, etc.
- **Environmental**
  The cloud can help organisations reduce the environmental impact of their data-centres, utilising renewable energy sources, or simply benefiting from centralised computing resources
- **Alternative Payment Models**
  Using a shared platform, helps move towards an OPEX model, instead of upfront capital investment

When we consider implementation, it should not be an "all or nothing" approach to moving services to the cloud. With any technology that breaks from traditional networks (and cloud technology is that to most people), there has to be easy transitional steps, moving only the solutions that make sense.

This is the reality for larger providers, but the challenge arises when less reputable or veracious companies want to join the cloud bandwagon, and the above points are compromised or neglected.

What can this mean? It has been "cloud providers" running applications on single servers in a single data centre. Please note, I use the term data centre loosely, an under-stair cupboard may be a better description. Data security is often compromised, as it's seen as a cost with no visible or immediate benefit.

The OPEX model hasn't been fully embraced either, with vendors still struggling with incremental billing and requiring upfront investment for three years despite no hardware, on-premise software or configuration required.

There have also been examples of service providers going out of business where the cloud technology was shut down or even held to ransom. With the importance of the application and more so your data, what contingencies would you have in place if this were to happen?

There are some real benefits to moving to the cloud, if done appropriately and with due diligence. It's essential to ask the right questions, and ensure you feel as secure as you would if the computers were on your own network.

FREE THE WAN!

IS YOUR CONNECTION READY FOR THE CLOUD?

Is your Wide Area Network infrastructure being held hostage?

It wasn't too long ago when choices in network connectivity were very limited. If a company wanted solid wide area network performance between corporate locations the choice was MPLS. The costs and limitations associated with MPLS had to be endured. Remote locations were relegated to second class citizenship in the WAN as MPLS connectivity was often cost prohibitive. Bandwidth in locations served by MPLS often lagged behind what was available in the open market. In exchange for this, companies often had to agree to long term contracts with their carriers.

Why would a company choose to endure this? With all of its short comings there were redeeming values to MPLS. Network performance on a MPLS network typically far exceeds that of an Internet native VPN. Security conscious companies enjoyed the added security provided by an MPLS network. Additionally, having a "single throat to choke" or outsourcing the entire WAN had its appeal.

Recent trends in the network have increased the strains on the WAN. With more burdens being placed on the WAN by feature rich connected applications and cloud applications, bandwidth is often at a premium in an MPLS network. Many companies are being limited in their IT initiative because of concerns about their wide area network. In many cases a simple MPLS upgrade is cost prohibitive. In others, concerns about network uptime has killed IT initiatives.

The drive towards cloud computing is the purest example of the challenge - it offers simplicity, efficiency, flexibility. But not without an internet connection…

IS YOUR MPLS ENOUGH TO HANDLE YOUR GROWING WIDE AREA NETWORKS NEEDS?

IS GROWTH IN CLOUD AND CONNECTED FEATURE RICH APPLICATIONS PUTTING ADDED STRESS ON YOUR THE WAN?

ARE MPLS UPGRADE COSTS PROHIBITIVE?

CAN WIDE AREA NETWORK CONCERNS LIMIT IT INITIATIVES?

IS GEOGRAPHY LIMITING YOUR NETWORK CHOICES?

Next Generation WAN Optimisation

The solution is WAN optimisation - whether you are resolving international, multi-site connectivity or simply maximising the efficiency of your interest connection and ensuring business continuity in the event of failure. Solutions are ISP agnostic, providing great flexibility in future connectivity.

What does this mean for the business?

- **Embracing VOIP** - session integrity, call dropping and inconsistent bandwidth is no longer a problem and allows for a complete move to UC.
- **Traffic Management** - ensuring high bandwidth to priority corporate applications
- **Forgetting MPLS** - by utilising multiple, more cost effective connections, expensive and inflexible MPLS can be consigned to history
- **Embrace Hybrid** - combine public and private internet options, physical and virtual networks, and lines from fibre to copper to wireless (3G, 4G and satellite)

FatPipe's next generation appliances allow applications at the premise gateway to be combined into a single appliance reducing your network footprint. WAN Optimisation, UTM functionality, Quality of Service, Network Monitoring, as well as Link and Server Load Balancing can be combined into a single high availability pair of appliances.

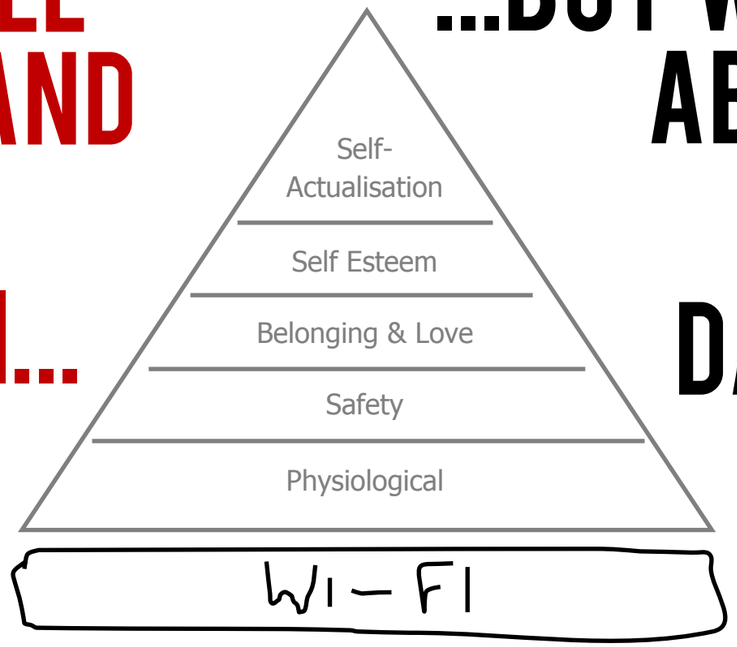
e92plus

FATPipe

Visit www.e92plus.com/Fatpipe to learn more

WE ALL DEMAND FREE WI-FI...

...BUT WHAT ABOUT THE DATA?



The need to track and trace users and store data is often an ignored requirement says Antony Byford, Head of Channel UK & Ireland at ZyXEL.

It's now a given that Wi-Fi access will be available in just about any public location. In hotels, on trains and when you visit a customer or supplier, you may be expected to provide log-details. Most of the time, no-one actually records who you are and where you are from. They will never really know what you are accessing or downloading or who you are communicating with across their connections.

With growing concerns over online security, particularly how criminals and terrorists are using the web to communicate, plan and even execute their attacks, the time is coming when organisations will no longer offer open access. It's already highly inadvisable, and can be illegal if unmonitored.

Tracking and tracing

Legislation from the EU already exists - the Data Retention Directive (DRD) - which requires communications providers to retain, for between six months and two years, data that would enable the relevant authorities to trace and identify the source and destination of any communication, as well as when it was made, its duration and type. It also required that providers should be able to identify the communication device and the location of mobile equipment.

Providers are expected to make the data available to competent national authorities on specific cases, "for the purpose of the investigation, detection and prosecution of serious crime." But while the Directive has been broadly adopted in a number of European countries, the UK decided that only comms providers that had more than around 500,000 subscribers would be forced to comply.

There are flaws in this legislation too. It would be difficult to trace someone who had accessed services though a public Wi-Fi hotspot, for example. But it won't be long before that particular issue is addressed. There are just so many hotspots now and it would be all too easy for individuals or groups with malicious intentions to simply move around from bar, to cafe to hotel, and make it much harder for the authorities to pull all the threads together.

Day of reckoning

A European Commission review of the DRD is underway already and it is highly probable that much more stringent rules will be imposed. The whole process could easily accelerate if some dramatic breach of security or data theft was to occur and, due to the laxity of the current rules, the perpetrators could not be traced.

Sooner or later, anyone offering guest Wi-Fi access will need to start thinking about how they can register and record all the details of users and authenticate them. If they want to get ahead of the game, they will start doing this now as it will soon become a requirement. It will, after all, be their IP address that is traced if there is a security concern or someone is doing something suspicious or illegal through their hotspot.

It is not that difficult to record guest information and the data; all you need to do is provide some form of data logging system.

Essential tools for compliance

Access Gateways, like the UAG4100 from ZyXEL, can help organisations deliver the essential free Wi-Fi that customers, guests and employees demand with minimal management and administration. It also provides the content filtering and web security needed to keep them secure, and avoid potentially embarrassing situations. It even allows for ticketing, billing and payment gateways for a premium or tiered service - ensuring customers get online and the business sees ROI. Ask us for your free evaluation.

SECURITY & NETWORKING MYTHS

Switches are not relevant for network security

In fact modern managed switches provide various security settings such as VLANs, Access control list or Radius authentication to avoid unauthorized network access and traffic flow in you internal network

The higher the port speed the better the data throughput

Besides the pure maximum port speed there are various settings in managed switches to prioritise the network traffic based on customer's requirements. So even lower port speeds can have a better data flow, if the settings are right.

Web-managed switches have less features than fully managed and are not as good

The main difference between web-managed and fully managed switches is the additional command line interface enabling text and script based configuration. Which is helpful for mass deployment and remote configuration or monitoring. Modern web-managed switches have almost the same features set and are sufficient for small or midsized networks.

Small businesses do not need a complex firewall

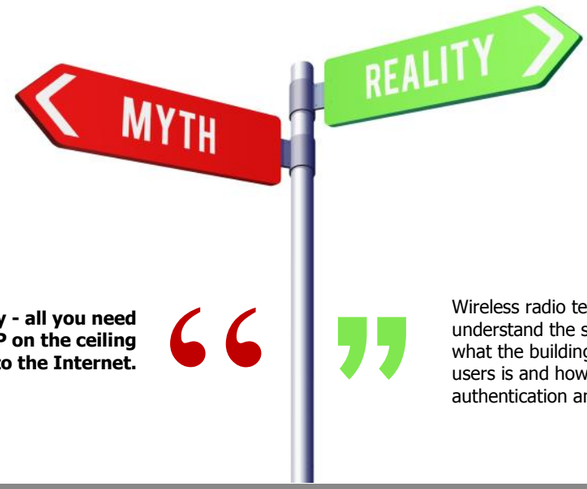
Malware attacks affect every network equally and small businesses especially can't afford a day of downtime!

With link aggregation you can increase the total port speed

Based on the communication protocols a switch always establishes a direct one to one communication between clients. So using link aggregation feature just gives you additional roads for the traffic. It does not make the road wider. By aggregating two Gigabit ports for an uplink we will get 2x 1GB but not 1x 2 GB. So the max speed stays the same but multiple clients can use it at the same time.

Remote access is difficult to implement

Hybrid VPN offers specified methods of remote access (IPsec, L2TP, SSL) and with ZyXEL´s EASY VPN the implementation is a walk in the park



Installing Wi-Fi is easy - all you need to do is install an AP on the ceiling and connect it to the Internet.

Wireless radio technology is not easy! You need to understand the signal strengths and signal radius, what the building is made of, what the density of users is and how to control and manage connections, authentication and bandwidth dynamically.

ZyXEL
Get more from your network - from the gateway to the core. Visit www.e92plus.com/ZyXEL for your free evaluation

TO ERR IS HUMAN, BUT SECURITY IS NOT FORGIVING

PROTECTING AGAINST USER VULNERABILITIES

Just last week, a colleague of mine told me about a break-in in his house. I was surprised, since I knew this person just recently invested in a digital home security system. However, he forgot to arm the security system when he left his house with the kids for the weekend game. Technological sophistication was no match to human error!

Likewise, information security technologies and systems have always been susceptible to human error. Mistakes happen due to negligence, ignorance, miscalculation, or a casual approach to security. Whatever the cause may be, these errors have a potential to pierce the technological layer of security and the resulting breaches can turn out to be expensive.

I spent several years working on Wi-Fi security and wireless intrusion prevention. Among the myriad of wireless attack vectors that I came across, many had some human error angle to them. Ignoring the certificate mismatch warning of the browser or typing in HTTP instead of HTTPS in the browser URL are the types of human errors that the Wi-Phishing attack vectors and tools like Wi-Fi Pineapple and SSL-Strip exploit. Keeping stale wireless network profiles in the client device from prior connections or an irresistible temptation to jump on a "Free WiFi" network can make users connect to untrusted wireless networks, potentially operated by malicious elements. These types of human actions expose wireless connections to MITM (man-in-the-middle) attacks, wherein the attacker can grab passwords and other sensitive information from the wireless connections of unwitting users. In enterprise networks, such actions also result in bypassing the security screening of the traffic enforced at the front end firewall.

Another type of vulnerability I have come across due to human missteps is employees and contractors installing their own personal Wi-Fi access points on the enterprise networks, not for malicious reasons, but as a matter of convenience.

REQUEST YOUR FREE WIRELESS NETWORK VULNERABILITY ASSESSMENT.

To help ensure your wireless network is secure and not compromised, AirTight Networks are offering an assessment.

As part of the only Wireless IPS solution rated 'Strong Positive' by Gartner, the assessment automates compliance scanning and reporting of rogue APs and wireless threats. We'll also create a wireless inventory, locate rogue devices and provide a full report.

These access points are called rogue APs and they open backdoors into enterprise networks behind the firewall. And then, there is the whole new concept of BYOD (Bring Your Own Device), where there are simply too many potential places for users to trip over - such as the loss of the device storing sensitive information, connecting infected devices to corporate assets, accidently sharing company information between business and personal apps, etc.

That raises the question: what can be done to prevent human error from compromising security? Unfortunately, our brain does not have the equivalent of raising 403 Forbidden Error alarm to detect and stop human negligence or miscalculations. So, human error is not completely avoidable. However, user education on security can go a long way in reducing this possibility. Technology can be deployed to monitor, detect and prevent effects of human error. Tools such as wireless intrusion prevention system (WIPS) can monitor, detect and block certain user behaviours such as connecting to untrusted networks and installing rogue APs, in addition to protecting your networks from malicious attacks. Client management tools such as MDM can be used to catch human errors in BYOD. In addition, always think in terms of multiple layers of security to reduce the chance of human error punching a hole in your security.

Anybody who preaches information security will always tell you that "people" are an important part of the overall security puzzle. Human error is one of the reasons why that is so.

Dr. Hemant Chaskar is Vice President for Technology and Innovation at AirTight Networks, Inc.

HAVE CYBER CRIMES BECOME VICTIMLESS?

THE REALITY OF IT SECURITY INSURANCE

Each year at the RSA conference there is a trend. It usually reflects the collective efforts of IT security firms in addressing specific new threats. This year however, the trend was a bleak one, with many companies acknowledging that they have lost the fight to protect their boundaries and are now looking for different ways to protect their business.

Many companies now view cyber security as the greatest risk to their business, with greater exposure to the threats comes a desire to mitigate the aftermath of a breach.

One different way to address the overwhelming security threat is to invest in a cyber-risk insurance policy. Cyber-risk insurance policies are growing in popularity with the business community who are understandably keen to reduce the exposure of any breach. However, cyber insurance is no different to any other form of insurance and there are pros and cons that business owners should consider carefully before investing.

From personal experience we believe that owning an insurance policy results in crimes becoming victimless. Our property is stolen, we make a claim, we receive compensation, we move on. So can cyber insurance make corporate breaches victimless?

Insurance will cover financial loss but it won't help address the overall impact on a business. The cost of remediation, negative company reputation, reduced consumer confidence and loss of competitive advantage are impossible to insure against.

Like any contract the devil is in the detail. If someone breaks in to our home it is easy to identify. Yet what if your corporate

network is attacked by a "trusted user"? Most policies do not cover what they define as deliberate or reckless acts, but aren't most attacks either deliberate or reckless in nature?

"The real concern with cyber-insurance is if it leads to a culture of complacency with regards to protecting our organisations from risk"

The experience of buying personal insurance teaches us that as long as we meet a minimum standard we will receive a pay out in the event of a loss but defining and maintaining minimum standards in corporate cyber-space is not that easy.

My advice is to first engage with the insurer to understand how they determine their minimum standards and to understand how often they assess the security threat landscape. If new threats occur that impact cover will they provide recommendations to you as a client? If a new threat is identified will they expect you to procure a solution to address it immediately?

Secondly, be sure to look out for uninsurable risks and exclusions to the policy.

Finally, I would always recommend engaging a qualified IT security provider to assist in the analysis of the insurance policy. A trusted adviser should also be able to ensure you exceed the security standards rather than simply complying.

Cyber insurance certainly has a part to play in mitigating the financial burden of a breach but we must ensure that it does not lead to an attitude of complacency.

There is no substitute for a robust security policy, staff awareness, and sufficient security technology to protect from risk. We should not be so quick to give up on our network security because we can all mitigate security risks.

Tim Ager is the Managing Director EMEA of Celestix Networks, the leader in Microsoft Security Appliances, authentication and secure remote access solutions.


e92plus
Absolute Software
AirTight NETWORKS
AVIRA
BRADFORD NETWORKS
celestix
COMODO
Cryoserver
FAT Pipe
NComputing
Lumension
IT Secured. Success Optimized.
purplewifi
SafeNet
UCOPIA COMMUNICATIONS
websense
XIRRUS
ZyXEL
www.e92plus.com +44 20 8274 7000 Tweet us @e92plus Argent Court, Hook Rise South, Surbiton, Surrey KT6 7NL
We're going to need a bigger firewall...