2016 Threat Predictions and Top Ten Cyber Security Tips To Keep You Safe

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.nntws.com

NNT™ SECURITY THROUGH SYSTEM INTEGRITY NOW PART OF netwrix

Precis

This whitepaper reviews and discusses the range of Cyber Security Threats predicted by analysts and vendors, including the NNT view on the outlook for 2016 and beyond.

The second part of the paper examines why all organizations continue to be at risk of being breached and presents a Top Ten of Cyber Security Safety Measures to mitigate this sustained threat.

2016 Cyber Security Threat Predictions: Analyst and Vendor Views

To begin with we consulted a number of expert sources. As with many of these prescient reports, conjecture and guesswork certainly play their part. That said, there is enough evidence based on current trends and previously observed activity to take all this very seriously indeed.

What does 2016 hold in store? NNT reviewed the predictions made by Trend, Gartner and Experian for Cyber Security

What Does Experian Think?

Chip & Pin won't stop payment card breaches (only 53% of IT Security Executives believe EMV cards will decrease the risk of a breach)

- Whilst we may have expected there to be some pessimism to the claims that Chip & Pin would represent an end to Credit Card theft, interestingly, 47% predict no discernible improvement at all, never mind any sort of total prevention

Attacks on Healthcare Institutions will increase (Healthcare Records worth 10 times that of Payment Card details)

- On today's black market, Healthcare records are worth up to 10 times more than stolen payment card details

- Healthcare providers have notoriously poor defenses. Current FBI warnings are in response to a bout of breaches including one leading provider who had 4.5 million records compromised

- Healthcare records are being used to fabricate insurance claims, purchase drugs and generate fake ID's. The lack of prevailing security and the rich source of personal data available, makes this a very attractive target for cyber criminals

Cyber conflicts between Enemy Nations will increasingly affect civilians as targets and consequence spreads

- Cyber war(s) between Enemy Nations are likely to include attacks on public facilities such as Airports, Hospitals and Government Facilities, together with other Critical National Infrastructure such as the Energy Network

- Attacks on National Infrastructure are more regular, from the early Stuxnet attack (designed to attack Iranian Nuclear Facilities) and the more recent disabling of Ukrainian cell networks, reportedly by Russian intelligence

Hacktivism will make a come back

- Hacktivism both corporate shaming and 'Cause-Based' will increase – considered the ultimate leveler

- From Ashley Madison to threats on ISIS. The apparent success of some of these initiatives is fuelling a renewed vigor for those wishing to further their cause.

> *"This puts lives at risk, and it is sickening to see such an act"*
>
> *Phil Lieberman, Cybersecurity Expert*

Figure 1: Dangerous Precedent? *The Hollywood Presbyterian Med Center paid a $17,000 ransom when hit with a Cyber Attack*

What Does Trend Think?

2016 will see an increase in online extortion

- 2016 has already seen examples of this, with a key instance concerning the LA Presbyterian Med Center. The fact that this was a relatively quick and easy *'Hack for Cash'* is driving this predicted trend, with more on this topic later. The LA Presbyterian Med Center attack speaks to both the targeting of Healthcare as well as the increase in Ransomware

> ***The assault on Hollywood Presbyterian occurred Feb. 5***, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices, said Chief Executive Allen Stefanek.
>
> The hacker demanded 40 bitcoin, the equivalent of about $17,000, he said.
>
> *"The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key,"* Stefanek said. *"In the best interest of restoring normal operations, we did this."*
>
> The hospital said it alerted authorities and was able to regain control of all its computer systems by Monday, with the assistance of technology experts.
> Phil Lieberman, a cybersecurity expert, said that, while ransomware attacks are common, targeting a medical institution is not.
>
> *"I have never heard of this kind of attack trying to shut down a hospital. This puts lives at risk, and it is sickening to see such an act,"* he said. *"Health management systems are beginning to tighten their security."*
>
> *http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html*

At least one consumer grade smart device will cause fatalities

- From Drones circling our no-fly zones to Medical Smart Devices used to transmit emergency care information, all of these are targets for cyber compromise and all occupy disturbingly close links to human lives

China will drive mobile malware growth to 20M by the end of 2016

- Growth in Mobile Malware is already accelerating way faster than traditional computer based Malware. Since the tracking of PC-Based malware incidents began in 1984, it took 20 years to grow to 20M instances. By contrast, we have seen Mobile Malware grow to these levels within 6 just years

Hacktivism will increase

- There is now a broad consensus over this with Trend agreeing with Experian that this will be a key issue in 2016

Little or no change in priority or investment at a corporate level

- Despite all of this, fewer than 50% of organizations will have dedicated IT protection specialists

But, Cybercrime legislation will become a Global Movement

- Nations around the world will inevitably conclude that it will be necessary to combine forces to both improve Cyber Protection as well as their ability to fight back

> ***"Healthcare records are worth up to 10 times more than stolen payment card details"***
>
> http://www.experian.com/blogs/data-breach/2015/11/30/hacktivism-and-more-predictions-for-the-data-breach-landscape-in-2016/

What Does Gartner Think?

The attack surface is changing all the time

- Contemporary threat environment is broadening with the advance of Shadow and Bimodal IT
- The means of enabling IT is changing. For example, the Marketing Department may well have their own IT assets beyond the IT teams reach

Mapping Visibility

- The better you understand what you have, the better able to protect and monitor it you will be. Conversely, IT assets that are overlooked and neglected with respect to Cyber Security will be all the more vulnerable to attack

DON'T focus too much on Zero Day Threats!

- 99.99% of exploits are based on vulnerabilities known for at least a year, and that this trend will continue through 2020! Last year's most prevalent malware '*Conficker*' is based on a 7 year old vulnerability within Windows. By now this should be mitigated as the norm but corners are still being cut when it comes to basic Cyber Security Best Practices such as System Hardening/Vulnerability Mitigation

Emphasis should be more on prevention than detection

- Continuing on from the previous point, more focus should be placed on the fundamentals of Cyber Protection before investing in emerging technologies

Known vulnerabilities will be sold on the black market more

- Where new vulnerabilities and exploits are discovered, the value of these is now well-understood with an established market. Any class of hacker will see value in possessing diverse and up to date vulnerability intelligence with '*off the shelf*' weaponry representing value for money compared to originating hacking technology

****

NNT Summary of 2016 Cyber Security Threat Predictions

The field of attack is broadening

- New lucrative and disruptive targets are identified, and those with a cause to promote seek to enter the arena

Organized crime will join the cyber-crime movement as it ceases to be the sole domain of the specialist hacker

- $17k quick and easy 'Hack for Cash' at LA Presbyterian Medical Center combined with the prevalence of malware on the black-market makes cyber crime suddenly accessible and attractive to the mainstream criminal fraternity

Apathy and Cost will remain as the primary blocks to Cyber Security

- "It won't happen to us" will persist within Corporations and Government

The litigants are circling!

- The stakes are going to be raised as more lawsuits are brought for damages relating to the loss of personal identifiable information

The Typical Mistakes Made by Most IT Teams and Why Corporate Cyber Security fails

So we all get sold on the need for Cyber Security defense measures and there is plenty of FUD (fear, uncertainty and doubt) used to amplify the urgency and acuteness of the need.

The difficulty when determining the right Cyber Security strategy for your organization and in turn, which technologies and products to use is not too dissimilar to assessing the market choices for keeping your body fit and healthy.

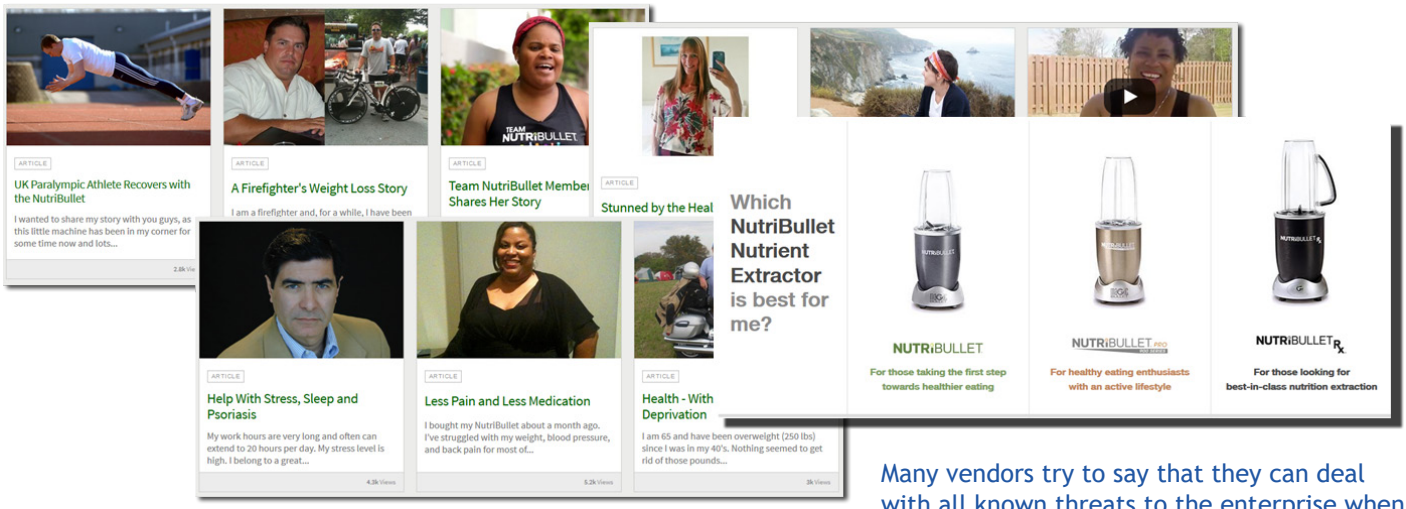


Figure 2: Drink this and you'll be cured! *The Cyber Security market, just like the health-remedy market, thrives on the promise of the 'new and improved' but also like the health-remedy market, maintaining comprehensive cyber security defenses takes more than just the latest gadget*

Many vendors try to say that they can deal with all known threats to the enterprise when actually, just like your personal health, it just isn't as simple as that. Cyber Security takes many forms and the range and nature of threat is so varied that there just isn't any getting away from the fact that it will require a multi-faceted solution.

But – it's easy to be tempted by the pitch! A sexy looking security appliance with a slick GUI is very tempting. And if it really can capture and defeat APTs, stop Phishing attacks and malware, block and alert on insider threats, hacktivism and rogue employees, while also protecting your IT from ransomware and government-sponsored/ blue chip espionage, then all your problems would be solved?

Likewise, if you really could lose weight, build a six pack and get marathon-beating stamina from drinking a kale and Persian cucumber milkshake, we would all do it. And of course, an anti-oxidant rich cocktail of vitamins and nutrients probably will help in some way, but it isn't going to get everyone losing weight and getting fit. In fact most would give it up and go back to bad habits.

Which brings us back to Cyber Security – it's also a 24/7 discipline and requires a combination of technology measures, procedures and working practices to maintain solid defenses.

And it is precisely for this reason that organizations will continue to get breached unless a Cyber Security mind-set becomes second nature for all employees.

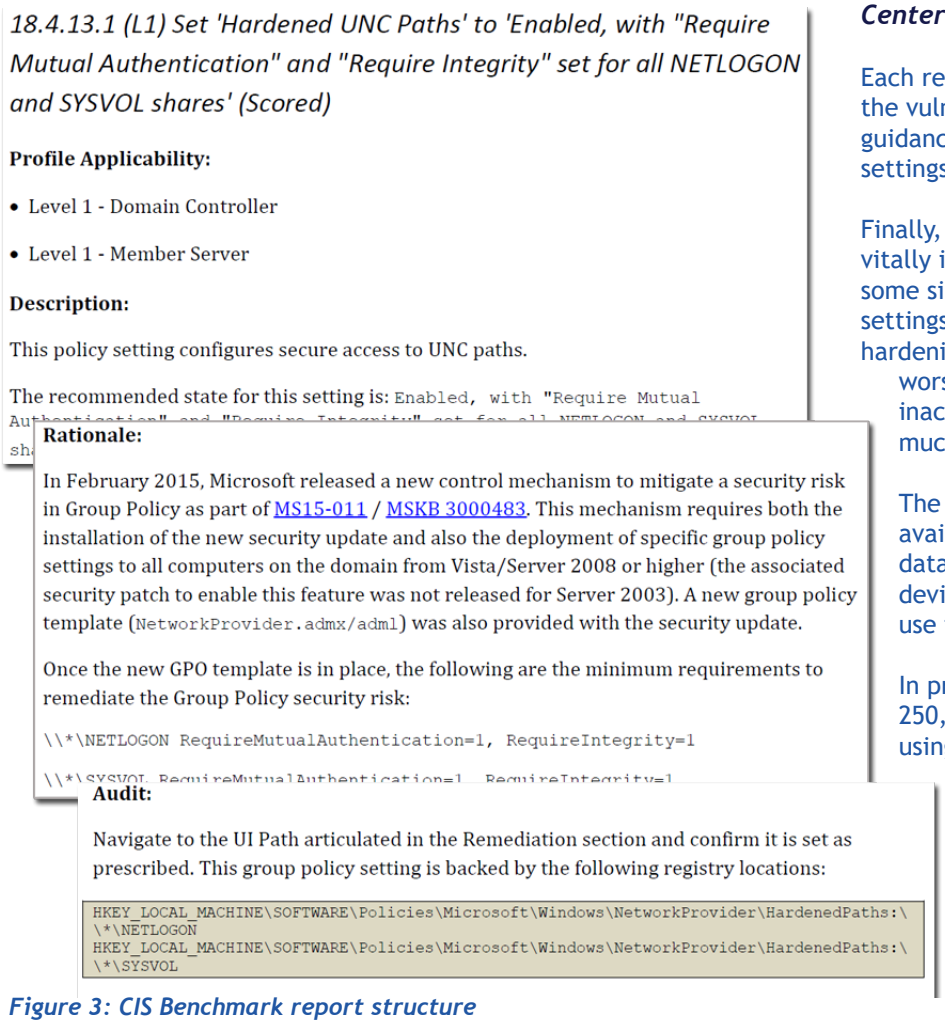
So, in the meantime, what should you be focusing on? Here's a quick summary – there are more comprehensive security policies, standards, and guidelines out there – see the PCI DSS V3.2 or any other GRC (Governance, Regulatory and Compliance standards), like NERC CIP, NIST 800-53 etc. There are also generic policies, like the SANS Top 20 or the CIS Security Policy that are freely available.

Top Ten Cyber Security Tips: 1. Mitigate Vulnerabilities

Easier said than done and most security policies duck out of providing specific prescriptive guidance, partly because this is a fluid area and the latest intelligence is always needed, but also because vulnerabilities need to be balanced against risk and operational requirements.

For example, most security professionals will tell you to minimize open ports and remove any unnecessary services, in particular FTP and Web Servers, so a typical hardening exercise involves disabling these. But if you actually need these for your application then you will need to balance security via other means.

The latest Microsoft Security Policy covers literally thousands of settings that control functional operation and in turn security of a host, so deriving the best balanced build standard can be a painstaking task. The Center for Internet Security Benchmarks provides secure configuration guidance drawn from manufacturers like Microsoft and RedHat, combined with academic and security researcher input. They are available free of charge and provide full details for auditing for and remediating vulnerabilities from a comprehensive range of platforms. This is an area where automated tools are definitely an essential.



18.4.13.1 (L1) Set 'Hardened UNC Paths' to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting configures secure access to UNC paths.

The recommended state for this setting is: `Enabled, with "Require Mutual Au... sh...`

Rationale:

In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (`NetworkProvider.admx/adml`) was also provided with the security update.

Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk:

`\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1`

`\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1`

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry locations:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\
\*\NETLOGON
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths:\
\*\SYSVOL
```

Figure 3: CIS Benchmark report structure

Center for Internet Security Benchmark Reports

Each report provides a ***Description*** and ***Rationale*** for the vulnerability, an ***Audit*** procedure and ***Remediation*** guidance, including any commands or Group Policy settings needed to eliminate the threat.

Finally, there will also be an ***Impact*** description, vitally important because there will almost always be some side-effects to consider when improving security settings, and the implications may not be obvious. Most hardening processes involve some trial and error, at worst, 'bricking' the device! (rendering it inaccessible/unusable - very secure, but no longer much use to the organization!).

The good news is that CIS Benchmark reports are available for a huge range of operating systems, databases, applications/middleware and network devices. Best of all, they are free to download and use for personal use.

In practice, given that there are often in excess of 250, fairly technical tests, the auditing is best done using a scanner or FIM tool so that the assessment can be done in seconds, even for many devices. Change Tracker Gen 7 provides not only CIS Benchmark auditing and reports, but for other standards too, such as DISA STIG, ISO 27K, NERC CIP and PCI DSS among others.

See more at https://benchmarks.cisecurity.org/membership/certified/nnt/

Top Ten Cyber Security Tips:
2. Firewall or better, IPS
3. AV
4. EMET
5. AppLocker

The best understood elements of any cyber security kitbag are the firewall and AV. They are fallible as we all know – zero day threats easily evade AV even while the AV is gobbling up system resources and more often than not, getting in the way.

Likewise, for the firewall or IPS - there are numerous ways to leapfrog the Firewall using phishing attacks, APT technology or just plain old Inside Help. However, outlined earlier, there isn't going to be a quick-fix, single-course of action or technology that will keep us secure, and these legacy security components still play an essential role.

Less well understood are some of the complementary technologies available that can be used to plug further weak spots. The market is awash with good ideas and exciting sounding technology. But before going to the market, you may well have overlooked what is available to you right now, valuable defense layers which are probably just not being used, namely EMET and AppLocker.

Both are Microsoft offerings, both free to use, and both requiring a little bit of know-how and experimentation to implement.

Enhanced Mitigation Experience Toolkit EMET provides a range of technical countermeasures to a variety of Windows vulnerabilities. This stuff really works to eliminate opportunities for malware through use of:

- ***DEP*** (Data Execution Prevention to block memory exploit malware)
- ***ALSR*** (Address Space Layout Randomization to prevent process hijacking)
- ***SEHOP*** (Structured Exception Handler Overwrite Protection defends against exception handler exploits, common to many browser exploits)

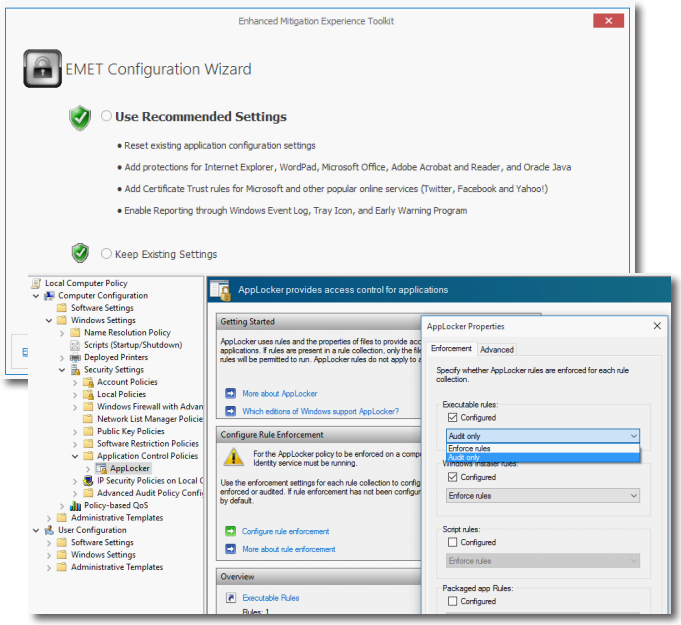


Figure 4: EMET and AppLocker are both free, but both provide active defense-measures for Windows systems

- ***Certificate Trust*** (aka Certificate Pinning to prevent Man-In-The-Middle attacks)
- ***Plus much, much more!***

EMET is provided as an optional extra and for good reason – it is very good at preventing malware execution, but this also means it will often break other applications. As with any hardening measure, test and introduce gradually. The default settings comprise Recommended and Maximum Security with the option to customize.

Download the software here https://technet.microsoft.com/en-us/security/jj653751

AppLocker AppLocker provides the means to whitelist/blacklist program and dll operation to lockdown PC and Server operation.

It is more of a blunt instrument in that it will stop programs dead in their tracks if in violation of your rules, so it pays to experiment with a willing user-group first!

For more https://technet.microsoft.com/en-us/library/ee424367%28v=ws.10%29.aspx

Top Ten Cyber Security Tips: 6. System Integrity Monitoring 7. Change Control – augmented with Threat Intelligence

There are three main reasons why change control and system integrity monitoring are vital to maintaining cyber security

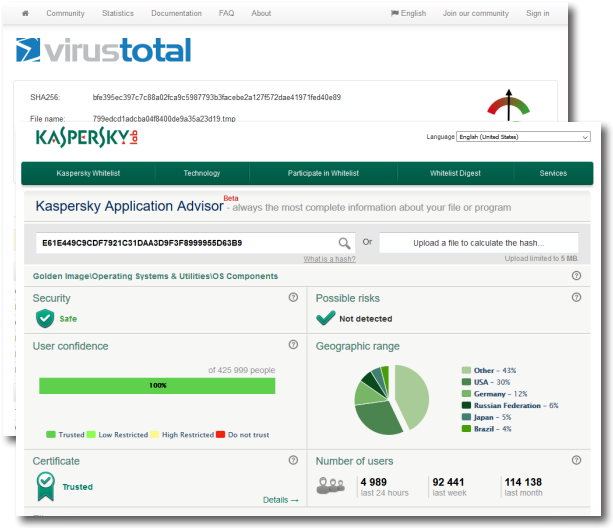


Figure 2: Various file whitelist repositories are available, providing a continuously updated, authoritative reference for 'known-safe' file versions

- Firstly, once our Vulnerability Mitigation and secure config work has been implemented, we now need that to remain in effect for ever more. So we need a means of assessing when changes are made to systems, and to understand what they are and if they weaken security

- Secondly, any change or update could impact functional operation, so it is vital we have visibility of any changes made

- And finally, if we can get visibility of changes as they happen – and especially if we have a means of reconciling these with details of known expected planned changes - then we have a highly sensitive breach detection mechanism to spot suspicious action when it happens

An intelligent FIM solution can be significantly enhanced by leveraging the encyclopaedic knowledge inherent in a whitelist repository. As changes are reported for review, the whitelist repository can provide the expert insight required to understand the file heritage and get a positive assurance that the file is 'known safe'.

Using Change Tracker Gen7, any gaps in the whitelist knowledge are plugged using Intelligent Change Control, with Gen7 continually improving its own whitelist of known-good change patterns and behaviors. Not only can the whitelist be queried manually when assessing the validity of a particular file, but can alternatively be used to automatically check each and every file change as it is detected.

All leading cyber security policies/standards call for change control and system integrity monitoring for all these reasons – it is key.

Top Ten Cyber Security Tips: 8. Promote an IT Security Policy

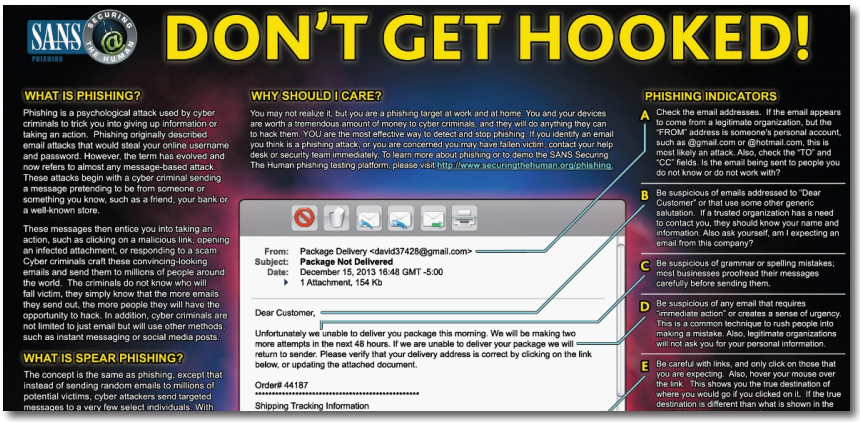


Figure 5: Cyber Security needs to be re-enforced organization-wide as everybody's responsibility - use these as Friday afternoon email flyers, lunch room posters and intranet landing pages to promote Cyber Security undersatnding within the organization

Promote an IT Security Policy Cyber Security isn't just the responsibility of the IT team and their security kit, but must be an organization-wide competence.

Children grow-up being taught about food hygiene - it isn't just the remit of professional chefs. Unfortunately, it takes generations for this kind of knowledge to become universally assimilated, so until Cyber Security hygiene becomes a basic life skill for all, it will be down to the workplace to educate.

To this end, in case your organization doesn't already have flyers/posters for Cyber Security education, there are plenty of resources available, again the SANS Institute provide a bunch of these that are free to use and very good see http://securingthehuman.sans.org/resources/posters

Top Ten Cyber Security Tips: 9. Encryption (BitLocker)

Encryption (BitLocker) Separate but related is the subject of data encryption – it slows everything down and gets in the way on a daily basis ***BUT*** it can prove a lifesaver if there is a breach that results in data theft. Loss of a company laptop is a pain but the loss of confidential data could result in anything from acute embarrassment to fines and lawsuits. Again, while plenty of commercial options exist there is also a free of charge MS option for this too in the form of BitLocker. You can use it to encrypt all drives or just data on local and removable drives.

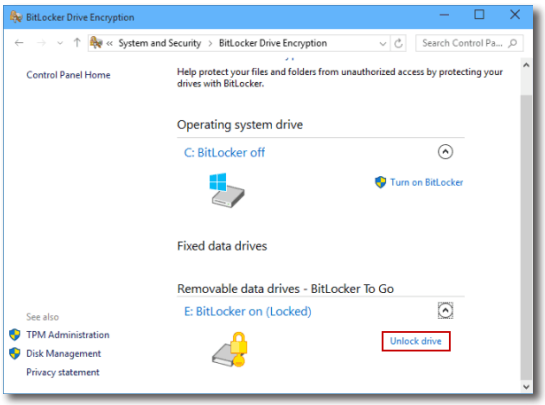


Figure 6: BitLocker selective encryption may prove to be a life-saver

In an enterprise environment this is controlled via Group Policy and as such, can also be audited automatically in the same way that vulnerabilities can be assessed. Used correctly, this same audit report can not only provide the recommended settings to use when first implementing BitLocker, but will also highlight any drift from your corporate build standard along with all other security settings needed to protect systems.

For more information on how to implement and use Bitlocker, see https://technet.microsoft.com/en-gb/library/dd835565%28v=ws.10%29.aspx

Top Ten Cyber Security Tips: 10. Finally - Don't be too thrown off course by the latest 'must-haves'

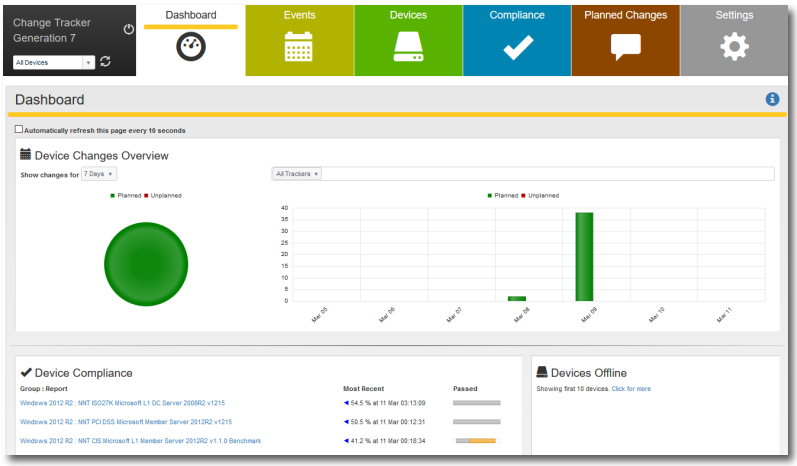


Figure 7: Automated technology like Change Tracker Gen 7 can drive security best-practice operation

The final piece of advice really is to focus on getting the fundamentals right and not chase the latest, niche or point products. If the maxim of *'there is no such thing as 100%'* security is accepted then how are you going to go about reaching a sufficient level of Cyber Security? The only answer is that it will need to be managed as a layered and 360 degree discipline, comprising technology and processes to first instigate and then maintain security.

Vulnerability Management, System Hardening, Change Control and Breach Detection are some of the absolutely essential components needed – the good news is that this can all be automated and just the 'need to know' exceptions reported for investigation.

Top Ten Cyber Security Tips: Final Word

Get your technology right for the general, everyday security before investing too much time and money into the latest 'hot' product.

- No such thing as 100% security
- No Magic Bullet (for cyber security or personal health)
- Cyber Security still requires a layered approach, and ~~is still hard work~~ ***MAY*** require some work :-)
- ***BUT*** it can be automated and made easier by good, automated technology

About NNT

NNT Change Tracker Gen provides continuous protection against known and emerging cyber security threats in an easy to use solution, offering true enterprise coverage through agent-based and agentless monitoring options.

- NNT analyzes every configurable component within your IT Estate and allows you to define a 'Known, Good, Secure and Compliant State' for all of your in scope systems.
- NNT-Change Tracker scans your devices and compares them to a standard policy, either user defined or based on an industry standard such as the Center for Internet Security (CIS).
- Policies can be automatically assigned based on the device type or priority via a centrally managed console.
- Gen7 is able to fully automate change approval for you, using the NNT FAST (File Approved-Safe technology) that combines unique intelligent change control knowledge base and whitelists.
- With NNT's real-time capabilities, unlike traditional scanning or exclusively agentless technologies, potential breaches to systems or policies are spotted immediately.

NNT Change Tracker Gen 7 helps you to prevent security breaches of your systems by providing you with a powerful feature-rich, easy to use and affordable solution for validating, achieving and maintaining compliance with corporate governance or security standards.

www.nntws.com

UK Office - Spectrum House, Dunstable Road, Redbourn, AL3 7PR
Tel: +44 8456 585 005

US Office - 9128 Strada Place, Suite 10115, Naples, Florida 34108
Tel: +1-888-898-0674

NNT Change Tracker Gen 7 - Real-Time, continuous FIM...and Certified by the Center for Internet Security

- Change Tracker Gen 7 has been certified by the CIS which means you can trust NNT to accurately deliver the most comprehensive, consensus-derived hardening checklists
- NNT provide CIS Benchmark checklist coverage for all Windows, Unix and Linux Operating Systems, SQL Server and Oracle Database Systems, and for Network Devices and appliances such as Cisco ASA firewalls
- Compliance is continuously enforced meaning vulnerabilities are highlighted more quickly than with traditional vulnerability scanners
- Better still, NNT Change Tracker Gen 7 provides continuous real-time FIM across all system, application, driver and configuration files providing peace of mind that system integrity is being maintained
- And if the worst case scenario does happen and your systems are breached or infected with malware, this will be detected within seconds, minimizing damage and costs

NNT Change Tracker is trusted by:

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com