Stop the Breach or Spot the Breach?

Closed-Loop Intelligent Change Control

It all CLICCs into place...

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

Abstract

Within any IT estate, the only constant is change.

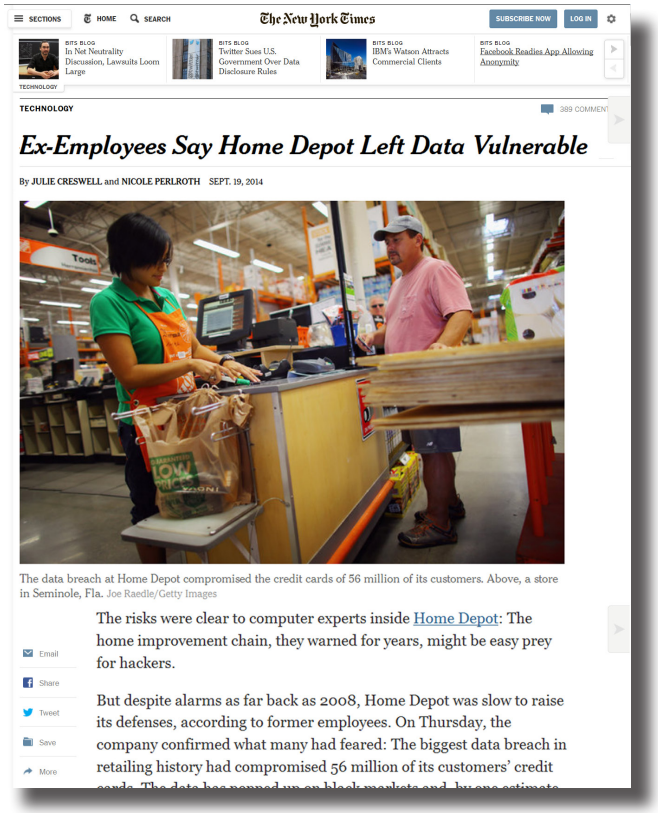
Change Control has always been a key security best practice. With every change made to IT systems comes a risk of a weakening of security defenses, not to mention operational problems, through misconfigurations. Changes also create 'noise' that makes it more difficult to detect a breach when a cyber attack succeeds.

With Change Control notoriously difficult to operate, especially at the forensic level of detail needed for security governance, a new approach is needed that gives the level of analysis necessary for breach detection. But how can this be provided without overloading already stretched IT Departments with yet more procedures to follow and alerts to review?

This white paper explores the need for file integrity monitoring-based change control and proposes a new approach to streamlining the review of security incidents and planned changes through automated, intelligent analysis.

When Will We Take Cyber Security Seriously?

How bad would an information security breach need to be in order to shock you? More to the point, how bad would a breach need to be for you and/or the Executive at your organization to take action?



The New York Times

SUBSCRIBE NOW LOG IN

BITS BLOG: In Net Neutrality Discussion, Lawsuits Loom Large

BITS BLOG: Twitter Sues U.S. Government Over Data Disclosure Rules

BITS BLOG: IBM's Watson Attracts Commercial Clients

BITS BLOG: Facebook Readies App Allowing Anonymity

TECHNOLOGY

389 COMMENTS

Ex-Employees Say Home Depot Left Data Vulnerable

By JULIE CRESWELL and NICOLE PERLROTH SEPT. 19, 2014

The data breach at Home Depot compromised the credit cards of 56 million of its customers. Above, a store in Seminole, Fla. Joe Raedle/Getty Images

The risks were clear to computer experts inside Home Depot: The home improvement chain, they warned for years, might be easy prey for hackers.

But despite alarms as far back as 2008, Home Depot was slow to raise its defenses, according to former employees. On Thursday, the company confirmed what many had feared: The biggest data breach in retailing history had compromised 56 million of its customers' credit

Email Share Tweet Save More

Figure 1: 'We sell hammers' - When will we take Information Security Seriously? If our Banks, Top Retailers and the Medical Establishment won't, what will it take to invoke a change of attitude to security?

It is hard to understand whether the regularity of major breaches, across all industries, is making information security a more critical issue or actually just deadening the impact. For too many of us, we hear of a breach, wait for the impact, and then – nothing.

However, if you are Target or Home Depot shopper, or if you bank with JP Morgan, or have received medical care from New York and Presbyterian Hospital, or especially if you work at one of these organizations, then you will now have first-hand experience of the worry, hassle, the drain of time and resources, and the horrendous costs that go with an information security breach.

If you haven't yet had to deal with the fallout from a major breach, then there may still be time to take the easy route. Because the fact is, it isn't inevitable that your organization will be breached. What is certain is that it is only a matter of time before you are subject to an attack. It is entirely down to your actions now whether that attack results in a destructive breach or not.

We all already know how to defend against cyber-attacks. You can be sure that within all of the organizations recently breached there was enough knowledge and capability to have either prevented the breach from happening, or certainly to have detected that an attack had resulted in a breach (maybe not at Home Depot with the 'we sell hammers' attitude).

Why do Breaches Continue to Happen?

So what is going wrong? In our experience, it's a mixture of a relaxed ***'it won't happen here, we have a firewall and some anti-virus software'*** attitude, through to a ***'we understand about IT Security Best Practices but we just don't have the time to operate them properly'***.

> ***"If the change is not one that was planned and expected, then it must be investigated as a critical security incident"***

For the first group thinking that firewalling and AV is enough, it is time to acquaint yourselves with the terms 'Security Controls' and 'Security Best Practices', then go back to the question asked at the beginning of this article.

For everyone else, you have our sympathy in terms of the amount of effort to properly operate a full spectrum of security best practices, but there is now a game changer when it comes to possibly the most challenging practice – change control.

Change Control – Easily the sexiest and most exciting dimension of Information Security (honest!)

Doing configuration management, change control or CCM (Change & Configuration Management) properly – especially from a perspective of maintaining security - has always been something easier done in theory rather than practice.

Any security auditor will tell you that you need a zero tolerance approach to unplanned changes in order to give yourself a chance of identifying a breach or malware infection. If the change is not one that was planned and expected then it must be investigated as a critical security incident (with the implication that will need an enterprise file integrity monitoring capability to detect changes as they are made – more on this later).

But is that realistic for all but either the smallest IT estates, where changes are fewand far between, or for the well-resourced Enterprise networks where there are enough personnel to dedicate the required time to policing change requests and then review the actual changes implemented? (apologies if you do fall into either of those categories, but you still don't have the time or resource to apply thorough change control to your changes!).

If you consider any of the breaches that have succeeded recently, change control would have made the difference between outright prevention or, at the very least, early detection. But if that is the case, why are the cyber attackers claiming more wins on the cyber-battlefield?

Six Sigma, ITIL, COBIT and Change Control – It's Just a Process of Elimination

The fundamental, 'process of elimination' is still the key tactic used for investigation and troubleshooting in any incident resolution/problem management initiatives. Incident and Problem are terms chosen carefully for their distinct definitions in service management frameworks such as ITIL and COBIT and their roles in other quality management programs, such as Six Sigma, and are both inextricably entwined with Change Control processes.

If you can find out what the difference is between before and after, uncover what changed and caused the failure, you can solve any incidents and resolve even complex, long-standing problems.

Six Sigma, ITIL, COBIT and Change Control – It's Just a Process of Elimination Continued...

Naturally enough, the more complex the system to analyze, the more difficult it becomes to apply this principle and this is why Change Management is often seen as a stifling bureaucratic process. Change Control rewards careful planning and preparation prior to changes being made with the focus heavily oriented towards contingency planning in the event of something going wrong after the change. The downside is that it needs careful planning and preparation, the paperwork and red tape that often makes Change Control a dirty word.

When change Control is employed as a security best practice, the emphasis is more towards having visibility of changes being made for two reasons. Firstly, by having clear sight of any changes being made, it becomes easier to isolate the unplanned, unexpected changes from the planned, intended changes, and to verify that changes have been properly implemented.

Mistakes made during planned maintenance can be identified, for example, hardening measures disabled on a host by an engineer making life easier for himself can be re-enabled before the vulnerable host is exploited. A simple typo in a config change can be picked up before problems arise.

Secondly, in a well-managed environment, any unplanned changes should be treated as potential security incidents. Where forensic-level change detection is employed, even the most subtle changes can be identified - hackers or Inside Man Attackers tend not to fill in RFC (Request For Change) forms. Malware from a phishing attack will be seen as an unexpected change and can be isolated before it spreads. For config based vulnerabilities, is it practical to mitigate the vulnerability, given that reducing the opportunity to exploit vulnerabilities invariably reduces functionality (for example, restricting RDP access makes a Windows server more secure, but would compromise support capabilities)?

It all CLICCs Into Place – Closed-Loop, Intelligent Change Control

But herein lies the crippling problem with Change Control – an overload of information to review and the burden of needing to pre-classify, identify and document changes in advance. Little wonder that Change Control is at best tolerated, but often resented in many IT Departments. All the same, if only tighter change control had been in force at Target (and likewise Home Depot) they could have saved a whole heap of trouble.

The numerous changes to POS system configurations including:

- New Services
- New DLL Files
- New Registry Keys

Provided all the clues needed to detect the breach and stop it dead in its tracks before it spread and set up residence, consuming over 40 Million payment card numbers within just two and a half weeks.

So in summary, to prevent breaches or at worst, detect them before they do serious damage, we need complete visibility of all changes being made and a means to review and verify them as legitimate planned changes, but without the associated resourcing overheads.

TARGET

"***What happened?***

In mid-December, we learned criminals forced their way into our system, gaining access to guest credit and debit card information. The investigation has recently determined that certain guest information was taken. That included names, mailing addresses, email addresses or phone numbers. We have partnered with a leading third-party forensics firm who is thoroughly investigating the breach

How many guests were affected by the additional stolen information?

Up to 70 million individuals may be affected.

How many credit or debit cards were impacted?

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013

source: target.com Jan 2014"

> **Closed-Loop, Intelligent, Change Control**...zero tolerance to unplanned changes...super-sensitive breach detection capability but without the time-consuming, resource-intensive (and boring) post-implementation review

It all CLICCs Into Place – Closed-Loop, Intelligent Change Control Continued...

Closed-Loop Intelligent Change Control, or CLICC, delivers just that.

CLICC reconciles the security benefits of forensic change control with the detailed workload necessary to review changes. The solution is 'Closed-Loop' and 'Intelligent', because any changes made are automatically assessed against expected or permitted changes to the configuration baseline, delivering all the benefits of zero tolerance to unplanned changes and a super-sensitive breach detection capability, but without the time-consuming, resource-intensive (and boring) post-implementation review hassle.

The most effective change control process requires fastidious review of the actual changes implemented compared to the expected and desired changes. In theory, when legitimate patches have been deployed, the inventory of changes made on one server will be the same as for all other similar servers. This goes hand in hand with the critical security best practice mentioned earlier, file integrity monitoring. By monitoring the filesystem of a host, firewall, or POS system, any changes to configuration files or system files can be detected and highlighted for review. FIM can also analyze configuration settings to ensure systems are configured in line with a corporate build standard, or even audited for compliance with a hardening checklist, such as those from the CIS.

Furthermore, any Trojan malware or other breach activity resulting in even tiny changes will be detected and in doing so, file integrity monitoring provides the perfect technology for host intrusion detection system operation.

Microsoft Patch Tuesday (there may be a slight delay...)

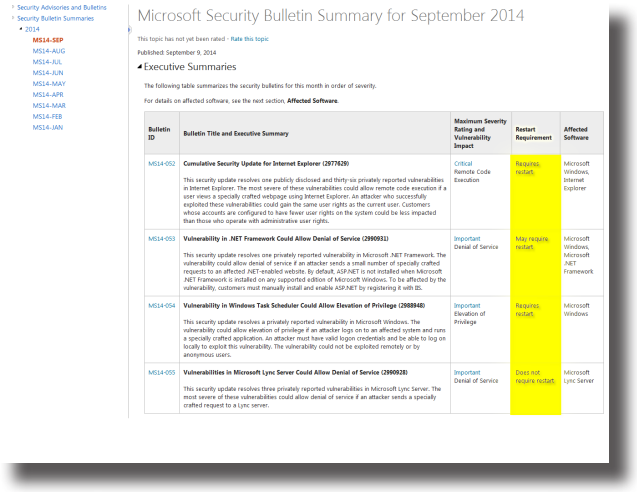


Figure 4: MS Patch Tuesday Bullettins are released to a chorus of groans around the world, and especially when the words 'Requires Restart' are included.

But all of this is easier said than done – there can be hundreds of files added or updated during patching, plus registry and security policy changes for Windows servers or POS systems. Microsoft's notorious Patch Tuesday releases signify groans around the world at the prospect of needing to deploy another bunch of patches estate-wide.

Manually verifying that the right changes have been made is simply not viable even on a small estate, let alone a major Enterprise estate. This is compounded by the classic update deployment problem in that it is impossible to predict when patches will be applied, especially those requiring a server restart. Servers may be offline, being re-built or too sensitive to patch automatically when patches are first published, prolonging the roll-out by days or even weeks.

This completely throws out the required tight orchestration of changes necessary in order to make forensic-level change control feasible.

So even if it was practical to assess which files and settings have been changed across an entire estate, the variable time window would make it a round the clock task to verify that changes were legitimate. The only realistic way to manage a secure estate is to restrict patching to once a month only and review a sample of servers using a file integrity monitoring tool – the traditional approach is to get the Tripwire ® Daily File Changes report and do a quick visual to see if there is anything out of the ordinary but nothing more scientific or exciting.

Closed Loop Intelligent Change Control Explained

However, if we know in advance the pattern of changes that are manifested by the patching exercise then we can effectively 'DNA Fingerprint' the exact details of the changes, right down to the secure hash value for the patched files, registry key value and security policy changes so we know we have got the correct patches and –
crucially from a security standpoint - only the correct patches, nothing else. This gives a patch image or blueprint, a template for the predicted changes expected to be seen across all similar systems. In fact, if we adopt a best practice approach to patching and first apply patches to a pre-staging test server, this can provide the basis for the template. In other words, the 'lab rat' test server used to verify that patches do not cause operational issues before a wide scale roll-out is instigated, also provides the 'donor' for the template under the CLICC approach.

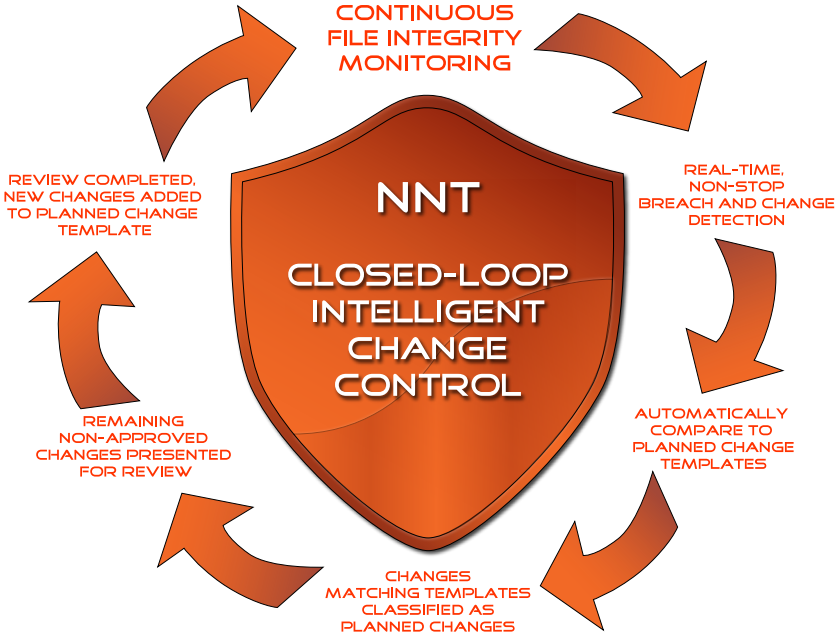


***Figure 5: Closed-Loop Intelligent Change Control** gives Information Security Teams an unfair advantage over hackers, malware and inside-man threats. By automatically assessing changes, all expected/pre-approved changes can be isolated leaving just unplanned changes - which may be breach activity - exposed, to then be properly investigated. Better still, all unplanned changes found to be legitimate can optionally be added to the list of pre-approved changes, improving the systems' intelligence further*

So to recap, all we now need to do is pre-stage our patches as in the regular patching process, extract the template of changes detected as a result of patching using our CLICC system, then roll-out patches as in the regular process. As patches are applied, the resulting file integrity changes to files, registry, security policy, databases, firewalls etc. will also be recorded by the CLICC-based file integrity monitoring system and intelligently assessed against the expected template.

Conversely, any other unexpected file integrity changes will be highlighted as potential security incidents, for example malware infecting a system or just some unauthorized system changes that could damage security or impair operational performance.

And because the CLICC system is intelligent, even if patches are delayed they will still be automatically reviewed and approved as permitted changes, but any other changes alerted as unplanned configuration drift for investigation and remediation. The CLICC system will improve its intelligence over time too, so as unplanned changes are investigated and found to be legitimate, these can be added to enhance the Planned Change Template to avoid further false positives in the future. Even if an un-patched server is brought on-line, as updates are applied these will be detected but as previously approved as OK changes, they will automatically be aligned with the original RFC - closed-loop means intelligence is improved and refined over time.

Consider that a well-run, secure operation will typically be patched in line with documented RFCs, there now exists the real opportunity to genuinely assess and approve all system changes as they are made, and detect any suspicious and unexpected activity. In reality, this may leave less than 1% of changes being detected in need of investigation and review, but now this can be done thoroughly without the 'noise' of legitimate changes cluttering up the Daily File Changes Report.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.