SysAdmin
Magazine

netwrix
2017

Assess Your Risks or Die Tryin’

30

SysAdmin
Magazine

№ 30 November ‘17

SysAdmin Magazine is a free source of knowledge for IT Pros who are eager to keep a tight grip on network security and do the job faster.

The Sysadmin Magazine team
sysadmin.magazine@netwrix.com

Contents

INTRODUCING **NETWRIX AUDITOR 9.5**

Identify, **Assess** and **Reduce Risks** to Your **IT Infrastructure** and **Data**

Download Free 20-Day Trial

Risk Assessment

Behavior Anomaly Discovery

Permission Analysis

API-Enabled Integrations

Ryan Brooks

Product Evangelist

What's New in Netwrix Auditor 9.5

Today, Netwrix Corporation released a new version of Netwrix Auditor, a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location.

The platform provides security intelligence to identify security holes, detect anomalies in user behavior and investigate threat patterns in time to prevent real damage.

A free trial of Netwrix Auditor 9.5 is available here

New capabilities available in Netwrix Auditor 9.5 include:

Risk Assessment

Organizations can detect, assess and remediate the security, governance and compliance gaps in their unique IT environments, so they can proactively reduce their attack surface and thereby minimize the ability of intruders and insiders to steal data or cause damage.

IT Risk Assessment: Overview

Gives you a bird's eye view of risks in your organization. Control and mitigate your IT risks by continuously monitoring and addressing weak points in your environment, such as chaotically organized privilege structure, "shadow" user and computer accounts, and improper content on your file shares.

Total risk level for Permissions: Acceptable

Risk	Level
User accounts with administrative privileges	Acceptable
Administrative groups	Acceptable
Empty security groups	Acceptable

Total risk level for Data: Take action

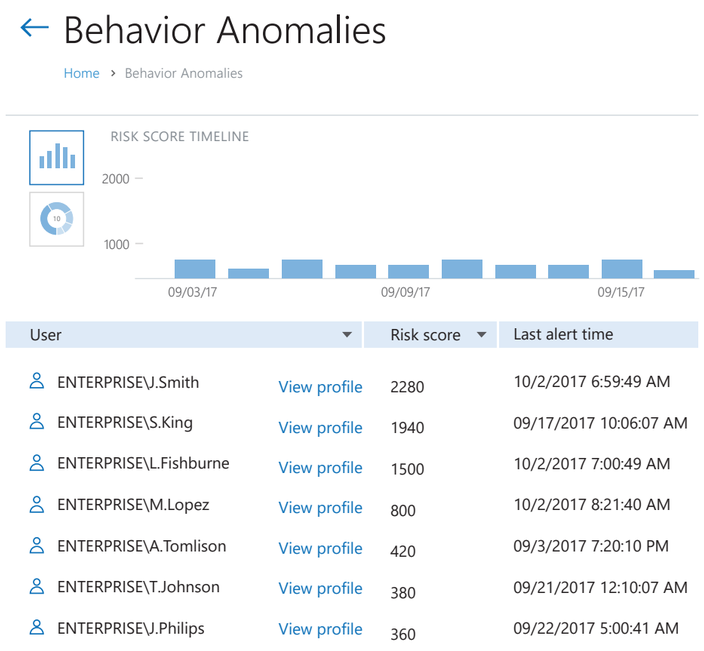
Risk	Level
Shared folders accessible by Everyone	Take action
File names containing sensitive data	Take action
Potentially harmful files on file shares	Take action
Direct permissions on files and folders	Pay attention

Total risk level for Users and Computers: Pay attention

Risk	Level
User accounts with Password never expires	Pay attention
User accounts with Password not required	Acceptable
Disabled computer accounts	Acceptable
Inactive user accounts	Acceptable
Inactive computer accounts	Acceptable

Behavior Anomaly Discovery

Customers can better detect rogue insiders and accounts compromised by external attackers with a single aggregated view of the anomalous activity by each individual. The associated risk scores enable them to prioritize incidents so they can investigate the most critical ones first and determine the best response.



Permissions Analysis in Active Directory & Windows Server

Customers can better detect rogue insiders and accounts compromised by external attackers with a single aggregated view of the anomalous activity by each individual. The associated risk scores enable them to prioritize incidents so they can investigate the most critical ones first and determine the best response.

New API-enabled Integrations

The Netwrix Add-on Store has been updated with three free, ready-to-use add-ons:

The Add-on for ServiceNow Incident Management uses information from Netwrix Auditor's alerts to automatically create detailed tickets in the ServiceNow ITSM and provide initial incident support for faster and more accurate incident investigation.

The Add-on for Privileged User Monitoring on Linux and Unix Systems enables better control over privileged activity on Linux and Unix systems.

The Add-on for Generic Linux Syslog provides a single-pane view of what's happening in the Linux environment, enabling customers to spot, investigate and block threats more effectively.

Try the upgraded Netwrix Auditor platform right now!

5 Things You Need to Know about IT Risk Assessment

With threats to sensitive data growing in both number and sophistication every day, organizations cannot afford a scattershot approach to security. Instead, they need to focus their limited IT budgets and resources on the specific vulnerabilities in their unique security posture. To do this, they need to identify, analyze and prioritize the risks to the confidentiality, integrity or availability of their data or information systems, based on both the likelihood of the event and the level of impact it would have on the business.

This process is called IT risk assessment. In this post, we'll reveal the five most important things to know about IT security risk assessment and implementing it in your IT environment.

1. IT risk assessment should be the foundation of your IT security strategy

First, we need to differentiate between risk assessment and risk management. While both are essential ingredients for a strong IT security ecosystem, they are not identical. Rather, risk management is a part of risk assessment, providing control over business, operational, information security and other risks. IT risk assessment involves the much broader task of understanding the internal and external risk landscapes for a holistic, organization-wide approach to security.

In other words, IT security risk assessment helps you understand what events can affect your organization in a negative way and what security gaps pose a threat to your critical information, so you can make better security decisions and take smarter proactive measures. For instance, by revealing a chaotically organized privilege structure, shadow user accounts or tangled administrative rights, risk assessment helps you take the proper risk management steps to minimize the risk of privilege abuse or data theft before it's too late.

2. IT risk assessment is required by many compliance regulations

The use of risk assessment for information security is only part of the picture. Information security risk assessment is also one of the top requirements of many compliance standards. For instance, if your organization must comply with HIPAA or could face GDPR audits starting May 2018, then information security risk assessment is a must-have for your organization in order to minimize the risk of noncompliance and huge fines.

Although regulations do not provide specific instructions on how organizations should control and protect their IT systems, they do require that organizations secure those systems and provide auditors with evidence that required security controls are in place and to reduce data security risks.

3. Adopting an appropriate framework makes it easier to get started with IT risk assessment

An IT security risk assessment framework is a set of rules that define:

- What has to be assessed
- Who has to be involved into risk assessment procedures
- What threats an organization has
- How these identified risks will be analyzed and prioritized
- How risk will be calculated based on likelihood and impact
- What documentation must be collected and produced as a result of the assessment

Obviously, these rules will be different for every organization, depending on its needs and goals, its size, the complexity and maturity of its business processes, the types of data involved, the size of the IT department, the security controls in place, the applicable industry requirements, and more.

However, there's no need to create your information security risk assessment framework from scratch. Instead, you can adopt and adapt one of these commonly used risk frameworks:

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) designed by Carnegie Melon University
- The NIST risk assessment framework, as documented in special publication SP 800-30
- ISO/IEC 27001:2013

Note that all of these standards require organizations to document their information security risk assessment processes so they can provide evidence that all required data security procedures are being diligently followed.

4. IT risk assessment needs to be an ongoing process

Security systems are like high-performance race cars — they need to be constantly maintained, updated and tuned. Risk assessment is not a one-time event that provides permanent and definitive information for decision makers to inform their responses to information security risks. Instead, because both the IT environment and the risk landscape are constantly changing, risk assessment needs to occur on an ongoing basis throughout the system development lifecycle, from system planning through acquisition and use to system retirement.

> **Security systems are like high-performance race cars — they need to be constantly maintained, updated and tuned**

Moreover, risk assessment has to be held frequently enough in order to spot potential security gaps that can arise quickly, such as privilege sprawl, inactive accounts and administrative accounts with improper password settings that put sensitive data and systems at risk.

5. IT risk assessment involves three stages

The process of risk assessment can be roughly divided into three stages:

- **Risk identification** — Determine the vulnerabilities in information systems and the broader IT environment, such as excessive access permissions or tangled group nesting, that could lead to damage if not taken care of in time.

- **Risk estimate** — Assess the likelihood that a risky event will occur by analyzing the probability that a given threat is capable of exploiting a given vulnerability.

- **Risk prioritization** — Rank risks based on the risk estimate combined with the level of impact that it would cause if it occurs. Consider the impact to the business of the unauthorized disclosure, modification or destruction of information, or the loss of information system availability. Attend to the threats with the highest probability and impact first.

IT risk assessment is critical to data protection and business continuity, and it has to be carried out periodically in order to detect new risks and improve security strategies. If your risk assessment is out of date, so are your strategies — it's as simple as that.

Find out what first steps to efficient risk assessment you can take right here.

Oleg Lalaev

AD Administrator

Active Directory Management: Top 7 Common Mistakes

Managing Active Directory is not an easy task, but someone has to do it. If this "someone" is you, then you should always keep in mind that human beings make mistakes, even if they are AD gurus.

To minimize the risk of such mistakes from happening on your watch, I'll walk you through the most common ones and help ensure that you never make them again.

Mistake #1

Using accounts with admin rights for everyday use

Don't use domain admin or even local domain accounts for login if you don't need such privileges. Use a normal account to log onto a machine and a privileged/admin account for elevated access. The reason for this separation is to avoid security breaches such as a spear phishing attack or malware injection while logged into the account with elevated credentials.

Mistake #2

Adding users to Domain Admins group instead of delegating access

Ignoring the concept of the least privilege is a major security issue. Consider a delegated Active Directory security model, especially for common administrative tasks such as unlocking accounts and resetting passwords. You need to carefully evaluate the job duties of everyone who needs to work with AD. Think about specific processes that can be automated. For example, the helpdesk role may include permissions to reset user passwords, connect computers to the domain, and modify certain security groups. Use AD Delegation Best Practices for more efficient management of AD delegation.

Mistake #3

Having poor backup/recovery plans

If someone deletes an Active Directory object, how quickly can you recover from this unauthorized change? Planning and testing recovery options are a must for all organizations to quickly recover from mistakes. Configure and use an AD tombstone or recycle bin to recover AD objects. Consider a delegated Active Directory security model, especially for common administrative tasks, such as unlocking accounts, and resetting passwords.

Mistake #4

Managing Active Directory from your domain controllers

This means that the administrator physically logs into a domain controller and launches the management tools from the server. This bad practice isn't limited to regular AD object management—it may also occur with Group Policy Management, DHCP, and DNS consoles. As best practices suggest, domain controllers should only run the roles required for domain services (which include the DNS role, but never use DC for DNS; always point it at another DC), and all daily administration should take place on protected administrative machines.

Mistake #5

Not terminating stale accounts

Stale accounts should be disabled and then deleted, because if you leave them untouched, a former employee or a malicious user can use them for data exfiltration. A healthy AD environment is a clean AD environment. When an administrator leaves stale users, computers, groups, or even GPOs around, they also unnecessarily complicate their environment.

Mistake #6

Having poor password policies in place

Before you pin the vulnerability of passwords on the bad habits of users, you may want to examine your policies compared to compliance and password best practices. Here are just a few tips:

- Never set a user's password to never expire.
- Set a service account's password to not expire, and then schedule a regular reset.
- Using the same password for multiple accounts means that an attacker has the master key as soon as he compromises one service.
- Use different passwords for your work, personal email, Facebook account, etc.
- Follow Password Best Practices to better manage passwords.

Mistake #7

No Active Directory auditing and monitoring

Monitor your AD health and quickly troubleshoot outages. Extend Event Log Size on your domain controller to maximum. Always track changes in your Active Directory, especially changes to the Domain Admins group. To track changes you need to enable audit policy; follow best practices to configure it properly. Tracking changes will definitely ease your investigation and troubleshooting process.

Ilia Sotnikov

IT Security Expert

Embrace Yourself, HIPAA Security Risk Assessment Is at Your Door

I'm horrified by the torture organizations go through to prepare for HIPAA audits. To help, I've put together the key concepts around risk analysis and the seven steps for getting started.

Do you work for a HIPAA-covered entity or business associate? Then you may be wondering exactly what IT risk assessment is required for HIPAA compliance, why organizations fail to do it properly, and where you should start to pass an upcoming HIPAA audit. Here you will find answers to these questions. Let's take it step by step.

HIPAA risk assessment: Everyone needs it, but nobody does it properly

IT risk assessment (or "risk analysis" as HIPAA refers to it) is one of the key requirements for HIPAA compliance. It is essential for protecting electronic protected health information (e-PHI) from various cyber threats. Failure to perform continuous security risk assessment can lead to data breaches and failed compliance audits, which in turn, can result in civil and criminal penalties — to get the idea, just look at the article headings in the news section of the website for the HHS Office for Civil Rights (OCR).

Unfortunately, both breach investigations and desk audits conducted by the OCR show that lack of proper IT risk assessment analysis and risk management is, and will continue to be, an issue for HIPAA-covered organizations. Even as on-site HIPAA audits approach, organizations struggle to establish enterprise-wide security risk analysis and respond with proper controls and procedures.

So, what's the hitch?

1. IT risk assessment must be continuous.
IT risk assessment is a complex, continuous process that requires skills and knowledge to be established and maintained. It is by no means a one-time, set-it–and-forget-it task.

2. There is no clear workflow. Because so many different types of organizations are subject to HIPAA compliance, the regulation lacks specific guidance on what risk assessment should consist of. Therefore, many organizations that need to comply with HIPAA don't even know where to start or whether they even understand IT risk assessment the same way OCR does.

What is risk assessment in the context of HIPAA?

According to HIPAA (§ 164.308), risk analysis is:

> **An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate**

Its purpose is to identify conditions where e-PHI could be disclosed without proper authorization, improperly modified, or made unavailable when needed.

The HIPAA Security Rule applies to all e-PHI that is created, received, maintained or transmitted by a HIPAA-covered entity, which includes business associates. Moreover, proper IT risk analysis must cover "all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes."

But even after we are done with all these definitions, it's still somewhat vague, isn't it?

Where to start with IT risk assessment

Since the HIPAA Security Rule doesn't provide exact guidance about what risk assessment must include, it is your responsibility to determine what scope of risk and security assessment would be comprehensive for your organization and how you can achieve it. Of course, risk assessment is such a huge area that you can't do everything it implies, regardless of your resources. Rather, you must be prepared to prove to auditors that you took all necessary and reasonable measures to protect your e-PHI by identifying risks, assessing their likelihood and impact, and addressing the ones with highest priority. You also need to have a persuasive explanation why certain measures are not appropriate for your environment and be able to show the alternatives you adopted.

HHS does offer a document called Guidance on Risk Analysis Requirements, which can give you an idea of what is expected from you from the auditors' point of view. It suggests including the following elements in your risk assessment:

1. Identify your e-PHI.

You need to find out what kind of e-PHI your organization deals with, where it is stored, and how it is received, maintained and transmitted. Note that sensitive data has a tendency to spread across multiple systems and applications; it is not necessarily only where you think it is.

2. Identify external sources of e-PHI.

If you work with partners or vendors with whom you share e-PHI, you should make a detailed list of all your data sources and make sure their security policies are in line with HIPAA.

3. Identify threats to e-PHI.

There are human, natural and environmental threats to information systems that contain sensitive data. There are plenty of ready-to-use forms that list threats. Find one online and use it as a starting point to reduce the risk of missing something important.

4. Determine the likelihood, impact and risk level of each threat.

The list of threats is long, so you have to prioritize your security efforts. Auditors will want proof that you worked hard to mitigate the most pressing risks.

5. Assess your current security measures and update them as needed.

Are your policies and controls sufficient to mitigate the risks you identified as high level? If not, update them to address current threats, and make sure they will also accommodate new circumstances and threats. Repeat this step on a regular basis. Adversaries are tireless and ever-innovative; do your best not to lag behind.

6. Document everything.

If it has not been documented, it never existed. You need to provide auditors with evidence of compliance for the past 6 years, including everything from risk assessment documentation to policies and log data. Just keep track of everything right from the beginning.

7. Never stop.

Make the risk assessment process continuous. Re-evaluate your risks every one to three years to ensure you are staying up to date in your efforts and practice.

Extra reading: The guidance document is largely based on the recommendations of the NIST framework, but it is a good idea to also familiarize yourself with the NIST framework itself. It will definitely be helpful in your compliance endeavors, as it offers an extensive list of IT risk assessment tasks and explanations of how to complete them, as well as a set of templates and examples. And, unlike the many other compliance materials that are vague and hard to follow, NIST is actually a pleasure to read.

Don't think you will be able to do everything required manually or in-house? There are many solutions on the market that can help. Just be aware that each solution covers only certain areas of compliance and risk assessment, and you need to find what suits your needs best.

Jeff Melnick

IT Security Expert, Blogger

Hot Tips: How to Harden Privileged Account Security

What are privileged accounts?

Privileged accounts are user accounts with extended permissions to access systems and data, such as the root account in Unix and Administrator accounts in Windows. Sometimes they are called "the keys to the kingdom" because a privileged account enables you do things ordinary users can't, such as change a system's configuration or view and delete sensitive data.

With such access at their fingertips, users can do either good or bad. It depends on who does what and why.

Do you have to worry about following best practices for managing privileged accounts?

If you have only five PCs, one router and a sysadmin with a lot of free time, you might not need to have rigorous privileged accounts management practices — but you are putting a lot of trust in that person. If you have a larger environment, you need to carefully follow best practices, both to ensure security and to meet compliance standards for maintaining a safe network.

To be able to hold privileged users accountable for their actions, it's essential to be able to answer the following questions:

- Who had access to a given system at a certain time?
- Who actually accessed the system and what specific actions were taken?

For example, suppose client information from your database is leaked to DarkNet. In the logs, you see that the Administrator account logged into SQL and copied the database — but because 10 individuals have the password for that account, there's no way to find exactly who did it. Moreover, without control over privileged accounts you can't be sure that it was even one of those 10 people, because any account could be compromised by a malicious insider or an external attacker.

How can you ensure privileged account security in AD?

- **Control access to resources** — Using Microsoft Active Directory groups is the best way to control access to resources and enforce a least-privilege model. It also enables you to easily enumerate permissions to any resource, whether it's a Windows file server or a SQL database.

- **Delegate control** — Delegation enables you to grant users or groups the permissions they need without adding them to privileged groups like Domain Admins and Account Operators. The simplest way to accomplish delegation is to use the Delegation of Control Wizard in the Microsoft Management Console (MMC) Active Directory Users and Computers (ADUC) snap-in.

- **Use strong passwords** — The Microsoft Active Directory Password Policy feature enables organizations to enforce the use of strong passwords through appropriate password and account lockout policies. You can even define different policies for different sets of users in a domain. You can enforce the use of strong passwords through an appropriate password policy GPO on your Windows Server; various settings enable you to control password complexity, lifetime and other requirements. For example, you can require admins to change their passwords regularly; ideally, the password should be changed automatically every time the account is used. (Read more about password policy best practices here.)

- **Enable auditing** — Windows audit policy defines what types of events are written in the Security logs of your Windows servers. Monitoring the creation and modification of objects helps you spot potential security problems, ensure user accountability, and provide evidence in the event of a security breach.

- **Configure NTFS permissions** — The main advantages of NTFS permissions are that they are based on the permissions granted to each individual user at the Windows logon, regardless of where the user is connecting from. (Find out more about NTFS permissions best practices here.)

- **Use user behavior analysis (UBA)** — Legacy defense strategies are typically focused on the perimeter, so they cannot identify insider threats or attacks in progress within the network. UBA delivers visibility into user activity across critical IT systems so you can spot these security issues. (See how Behavior Anomaly Discovery offered by Netwrix Auditor can help you improve detection of malicious insiders and compromised accounts.)

What else you can do?

Third-party solutions can help you implement the controls and policies you need to improve security for privileged accounts. In particular, account management security solutions can help you accurately provision and de-provision privileged accounts, and password vaults can store privileged credentials securely. Are you ready to take a step further? Here are efficient best practices you can follow to take control over privilege users across your IT environment.

Free Tool
of the Month

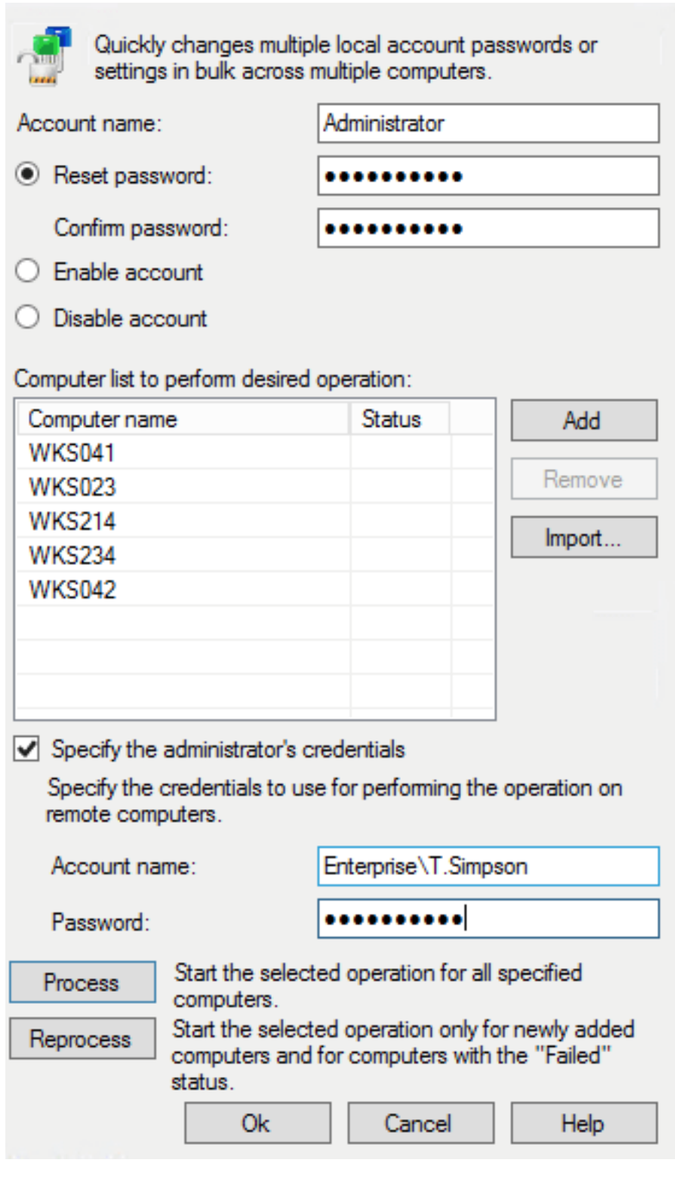
Bulk Password Reset

Download Free Tool

Reset Local Admin Passwords in Bulk with One Click

Freeware tool that simultaneously resets multiple local admin and user passwords, so you can strengthen security and automate password resets on your Windows Servers and computers.

- Reset administrator passwords in bulk
- Better manage your local accounts
- Minimize the risk of an attack
- Increase IT team productivity
- Ensure compliance
- Get it free of charge



How-to for IT Pro

How to Find Permission Changes across File Servers

1. Navigate to the file share, right-click it and select "Properties" > Go to the "Security" tab > Click the "Advanced" button > Go to the "Auditing" tab > Click the "Add" button > Select the following:

   - Principal: "Everyone"
   - Type: "All"
   - Applies to: "This folder, subfolders and files"
   - Advanced Permissions: "Delete subfolders and files" and "Delete".

2. Run gpedit.msc, and create and edit a new GPO > Go to "Computer Configuration" > Open "Policies" > Navigate to "Windows Settings" > Select "Security Settings" > Go to "Local Policies" > Select "Audit Policy" > Under "Audit object access", select the "Success" and "Failure" checkboxes.

3. Go to "Advanced Audit Policy Configuration" > Select "Audit Policies" > Choose "Object Access" > Under "Audit File System", select the "Success" and "Failure" checkboxes > Under "Audit Handle Manipulation", select the "Success" and "Failure" checkboxes.

4. Link the new GPO to file server and force Group Policy update.

5. Open the Powershell ISE Create a new script with the following code and run it, specifying the name of your file server and changing the timeframe if needed (86400000ms covers the last 24 hours):

```
Get-WinEvent -ComputerName fs1 -LogName
Security -FilterXPath "*[System[EventID=4670 and
TimeCreated[timediff(@SystemTime) <= 86400000]]
and EventData[Data[@Name='ObjectType']='File']]" |
fl | Out-File c:\data\permission_c.txt
```

Netwrix Auditor 9.5

netwrix.com/auditor9.5html

Corporate Headquarters:
300 Spectrum Center Drive,
Suite 200 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749
EMEA: +44 (0) 203-318-02