Most companies failing at cybersecurity metrics

- More than half of respondents (58%) scored a failing grade when evaluating their efforts to measure their cybersecurity investments and performance against best practices.
- 4 out of 5 companies worldwide are not fully satisfied with their cybersecurity metrics.

Failures in planning

- 1 in 3 companies invest in cybersecurity technologies without any way to measure their value or effectiveness.
- 4 out of 5 fail to include business stakeholders in cybersecurity investment decisions.
- 4 out of 5 companies don’t know where their sensitive data is located, and how to secure it.

Failures in performance

- 2 out of 3 companies don’t fully measure whether their disaster recovery will work as planned.
- 4 out of 5 never measure the success of security training investments.
- While 80% of breaches involve stolen or weak credentials* 60% of companies still do not adequately protect privileged accounts---their keys to the kingdom.

*2017 Verizon Data Breach Investigations Report
TABLE OF CONTENTS

Executive Summary......................................................................................................3

Introduction – The shameful state of cybersecurity metrics..........................................5

• Most organizations failing at measuring effectiveness of cybersecurity investments and performance
• Vast majority of organizations not fully satisfied with their cybersecurity metrics
• Lack of measurement leaves companies in the dark

Section 1 - Failures in Planning......................................................................................7

• Not measuring value of cybersecurity investments
• Not understanding what information to protect
• Not engaging key business stakeholders

Section 2 - Failures in Performance ..............................................................................9

• Not measuring expected outcomes
• Not measuring security awareness
• Not measuring compliance with policies or regulations

Section 3 - Lack of resources cited as major hurdle.......................................................12

Section 4 - Small businesses especially vulnerable.......................................................13

Section 5 - Recommendations.......................................................................................13

Appendix A – Survey Methodology/Demographics......................................................17

Appendix B – Free Resources.......................................................................................18
EXECUTIVE SUMMARY

THE 2017 STATE OF CYBERSECURITY METRICS ANNUAL REPORT

Results from this Security Measurement Index benchmark survey clearly indicate that companies need to do a better job of measuring business success and key metrics on how cybersecurity investments are performing.

KEY FINDINGS:

MOST COMPANIES FAILING AT CYBERSECURITY METRICS

With over 400 global business and security executives participating in this benchmark survey, more than half of respondents scored an “F” or “D” grade when evaluating their efforts to measure their cybersecurity investments and performance against best practices. Based on internationally accepted standards for security embodied in ISO 27001, as well as best practices from industry experts and professional associations, the Security Measurement Index benchmark survey provides a comprehensive way to define how well an organization is measuring the effectiveness of its IT security.

• 58 percent of companies are failing in their efforts to measure the effectiveness of their cybersecurity investments and performance against best practices.

Most survey respondents do not feel confident about how they are measuring the value of their cybersecurity investments, and 80% stated that they are not fully satisfied with the metrics available.

• 4 out of 5 companies worldwide are not fully satisfied with their cybersecurity metrics.

FAILURES IN PLANNING

With global companies and governments spending more than $100 billion a year on cybersecurity defenses, a substantial number---32 percent---of companies are making business decisions and purchasing cyber security technology blindly.

Even more disturbing, over 80 percent of respondents fail to include business users in making cyber security purchase decisions, nor have they established a steering committee to evaluate the business impact and risks associated with cybersecurity investments.

• 1 in 3 companies invest in cybersecurity technologies without any way to measure their value or effectiveness.

• 4 out 5 companies don’t know where their sensitive data is located, and how to secure it.

• 4 out of 5 fail to communicate effectively with business stakeholders and include them in cybersecurity investment decisions.

FAILURES IN PERFORMANCE

With Ransomware causing major havoc in the past year, it’s alarming that so many organizations are uncertain whether they have backed up information properly and if they can recover it in a timely manner. Nearly two out of three businesses (64%) among survey respondents fail to recover timely, or in away that aligned with their disaster recovery plan.
In addition, 8 out 10 companies fail to ensure that their IT security policies are understood by employees and measure this. This puts organizations at risk since human error or malicious intention are frequent causes of security breaches.

Access controls for privileged accounts in network systems are some of the most important ways to protect enterprises, including highly sensitive power accounts like those of a system administrator or root accounts that if compromised, can enable an attacker to move anywhere within the network undetected. Yet, nearly two out of three or 60 percent of our survey respondents fail to adequately protect privileged administrator accounts.

• 2 out of 3 companies don’t fully measure whether their disaster recovery will work as planned
• 4 out of 5 never measure the success of security training investments
• While 80% of breaches involve stolen or weak credentials* 60% of companies still do not adequately protect privileged accounts---their keys to the kingdom.

SMALL BUSINESSES ESPECIALLY VULNERABLE

Small and medium size businesses (SMBs) are being targeted more because their cyber security is typically much easier to compromise. Though they are not usually the main target but a secondary victim, the real goal of cyber criminals is to infiltrate partnerships SMBs have established with larger organizations via a supply chain or data shared with larger companies.

• Small businesses targeted in 2 out of 3 cyberattacks
• 60% go out of business six months after a breach

RECOMMENDATIONS

Results of the survey clearly indicate that cyber security metrics must become much more of a priority than they have been in the past. It appears that many organizations are making security decisions blindly without clear measurements about the impact on their cyber security posture, protect sensitive data, and ensure the business can recover efficiently from a breach. Most of all, enterprises must improve their efforts to collaborate with their business users to effectively secure their operations.

Educate
• Educate Employees and Measure Cyber Hygiene
• Mandate that C-Level execs experience a Red Team assessment
• Implement “Least Privilege” approach and culture

Protect
• Backup critical data and systems and customize your recovery plan for different types of cyber threats. Test your restore capabilities.
• Ensure Multi-Factor Authentication is in place
• Strengthen Identity Access Management and Protect Privileged Accounts
• Prepare and Implement a Cyber Incident Plan

Monitor
• Control, Monitor and Report Admin privileged access to systems
• Correlate, monitor and audit Security Logs

Measure
• Get your Key Business Metrics Sorted
• Take the Security Measurement Index Benchmark Survey
• Take the Password Management Benchmark Survey
THYCOTIC | THE 2017 STATE OF CYBERSECURITY METRICS ANNUAL REPORT

THE 2017 STATE OF CYBERSECURITY METRICS ANNUAL REPORT

SECURITY METRICS CAN HELP YOUR BUSINESS SURVIVE A CYBER-ATTACK – ARE YOUR SECURITY METRICS IN ORDER?

Results from this Security Measurement Index benchmark survey clearly indicate that companies need to do a better job of measuring business success and key metrics on how cybersecurity investments are performing.

INTRODUCTION: THE SHAMEFUL STATE OF CYBERSECURITY METRICS

This first State of Cybersecurity Metrics Annual Report reveals that more than half of respondents scored an “F” or a “D” grade when evaluating their efforts to measure their cybersecurity investments and performance against best practices. Based on internationally accepted standards for security embodied in ISO 27001, as well as best practices from industry experts and professional associations, the Security Measurement Index provides a comprehensive way to define how well an organization is measuring the effectiveness of its IT security.

More than half of companies worldwide (58%) are failing to effectively measure their cybersecurity investments and performance.

50% scored an “F”
8% scored a “D”
11% scored a “C”
13% scored a “B”
18% scored an “A”

With over 400 global business and security executives participating in this benchmark survey, most do not feel confident about how they are measuring the value of their cybersecurity investments. And 80% of survey respondents stated that they are not fully satisfied with the metrics available.
80% of companies worldwide are not fully satisfied with their security metrics

Question: Our security metrics help us evaluate real progress in our security posture.

No - 7%
Not Really - 30%
Mostly - 43%
Fully - 20%

In short, companies do not have the crucial security metrics in place to ensure they are making the right business decisions that are vital to growing their businesses securely.

According to survey participants, 37 percent of companies lack any kind of visibility into cyber security metrics. Another 43 percent of respondents indicated some visibility into cyber security metrics but still fail to integrate business stakeholder needs when making critical decisions.

The following report provides a snapshot of how companies are struggling with measuring their cybersecurity efforts. It focuses on two major areas: Failures at building in metrics at the planning stages of cybersecurity development, and failures in performance measurements of cybersecurity programs and products.

Why this cybersecurity metrics survey now?

Numbers are critical components of our digital world. They enable us to mathematically track, count, measure, label, and value the world in which we conduct our lives. It is bits and bytes that make our connected world function, determine how data gets from one place to another, and how we measure progress.

Numbers are key to tracking business value and risk: two critical key metrics when determining how much cyber security we need to protect our businesses and reduce the risk of breaches that threaten our privacy and commerce. This survey is designed to directly address how we measure the success of our defense against cyber threats.

To see how you measure up, take the survey at thycotic.com/cybersecuritymetrics You'll receive an immediate “grade” and a follow up email with a report that shows your responses compared with your peers.
SECTION 1 - FAILURES IN CYBERSECURITY PLANNING METRICS

LACK OF SECURITY MEASUREMENT LEAVES COMPANIES IN THE DARK

This landmark report helps to highlight several disturbing implications. With global companies and governments spending more than $100 billion a year on cybersecurity defenses, a substantial number---34 percent---of companies are making business decisions and purchasing cyber security technology blindly. These companies simply don’t possess sufficient data to know whether their investment decisions are actually making a difference in improving their overall cyber security posture.

34% of businesses are investing in cyber security blindly

Question: Our security metrics help us determine the resources we need to apply to our security program.

- No - 7%
- Not Really - 27%
- Mostly - 44%
- Fully - 22%

Perhaps an even more alarming survey result indicates that 80 percent of companies fail to discover and track sensitive data, nor do they determine where their critical data gets duplicated, and where it moves across their networks.

Many regulations require companies to provide adequate security and encryption for sensitive data like financial details, medical and contact data. Data Privacy is also a major concern globally as illustrated by the upcoming enforcement of the EU General Data Protection Regulation or GDPR, designed to protect the personal identifiable information of EU citizens.

In view of these regulations, and the high cost of cyber security breaches, it’s imperative that global organizations be able to discover and classify data critical to their businesses, and implement security controls to protect that information. But without knowing where their most sensitive data resides and how it moves across the network, companies will find it near impossible to measure the effectiveness of their cybersecurity investments.

80% of companies do not know where their most sensitive data is located or how securely it’s protected
Many organizations have created “Cyber Ambassadors” or “Cyber Advisors” to act as cross-departmental advisors to help manage cybersecurity. They aim to establish a “four eyes approach” that ensures someone will be responsible for identifying suspicious activity and managing security incidents. Ad hoc steering committees led by cyber advisors have also been formed in some cases to help determine the risks of implementing new technology solutions. Yet, according to this survey 83 percent of respondents fail to include business users in making cyber security purchase decisions, nor have they established a steering committee to evaluate the business impact and risks associated with cybersecurity investments.

83% of companies fail to fully include business impact in cyber security decisions

Question: Our company has a security steering committee with designated security representatives in business units and measures that security efforts are successful and expenditures are aligned with business objectives

Unfortunately, IT security teams often speak a very different language compared to that of their business leader counterparts. It’s a rare security professional who can easily translate security risks into terms that business users can readily understand. The CxO typically hears buzz words such as cyber-attacks, data leaks, credential theft, identity theft, malicious malware, ransomware or data poisoning. But in too many situations, IT security fails to understand or explain how various cybersecurity processes and technologies will impact and/or enable the business.

- Fully in place with measurements - 17%
- Partially in place with measurements - 26%
- Planned - 18%
- Not in place, measured or planned - 33%
- Not applicable - 6%

Partially in place with measurements - 26%
Planned - 18%
Not in place, measured or planned - 33%
Not applicable - 6%
Fully in place with measurements - 17%
IT SECURITY OFTEN SPEAKS A DIFFERENT LANGUAGE THAN BUSINESS LEADERS

This lack of communication and awareness among key leaders is especially concerning at the boardroom level, where business decisions are measured in contribution to the top and bottom lines. In stark contrast, the security team may well be measured by how well the firewall is performing yet have little comprehension of the business costs should a firewall fail, exposing the business to hackers. More than one-third of survey respondents or 34 percent simply have no idea if and how cybersecurity investments are aligned with business values and objectives.

This lack of business impact understanding and security metrics means far too many companies:

• Fail to effectively communicate performance or drive performance improvement
• Fail to measure the effectiveness of IT controls
• Fail to diagnose or prioritize problems
• Fail to guide resource and investment allocation
• Fail to demonstrate compliance
• Fail to communicate an accurate state of security to the board of directors
• Fail to prepare the business to respond to a cyber-attack and survive

Most businesses fail or suffer significant losses not because they have experienced a breach but because they are unable to respond to a cybersecurity incident promptly and effectively. They simply do not have the information or the metrics in place to help contain, reduce, and remediate rapidly evolving, sophisticated threats to today’s enterprises.

Securing an adequate defense against cyber threats depends on involving all stakeholders in making decisions, identifying the key assets to protect and how they are used, and then applying security metrics to help evaluate and improve the effectiveness of cybersecurity.

SECTION 2 - FAILURES IN MEASURING CYBERSECURITY PERFORMANCE

MEASURING AWARENESS OF CYBERSECURITY POLICIES AT THE “WEAKEST LINK”

While we constantly hear that cybersecurity is only as good as its weakest link---and all too often that weakest point is a human being clicking on a link that downloads a piece of malware or unintentionally giving up a password. While many incidents result from human error we must remember that the employee at this point is also a victim of the cyber-attacks.

But, according to our survey respondents, 8 out 10 companies fail to ensure that their IT security policies are understood by employees and measure this. This puts organizations at risk since human error or malicious intention are frequent causes of security breaches.

8 out of 10 organizations worldwide do not measure whether employees have read and understand what’s expected to enforce their company’s security policies
The survey indicates a general lack of responsibility and accountability to ensure employees/users clearly understand an organization’s cyber security policies. With the increasing presence of cybersecurity regulations and controls, developing well-defined IT Security Policies is typically a first step for most organizations — and one that must be endorsed from the top of the organization.

Ensuring that employees are well informed and that the IT security policies are clearly communicated to employees is an obvious first step in reducing the risk against both external and internal threats against an organization. All employees need to recognize how their behavior affects security and therefore treat security measures as an important part of their job.

80% don’t measure the success of security awareness training and cyber hygiene

Many companies in recent years have taken the initiative to develop cyber hygiene programs that help employees gain a better understanding of cyber security threats and how to best protect against cyber threats. However, in implementing these programs many companies fail to measure their success in terms of effectiveness. All too often cyber hygiene can revert a checkbox item that asserts, “yep we do that, we have cyber hygiene.” Rather than a one-time only task, cyber hygiene should be regarded as continuous learning and should be measured consistently to ensure that it genuinely makes a difference in helping identify and prevent cyber-attacks.

COMPANIES FAILING TO MEASURE DISASTER RECOVERY CAPABILITIES

64% of organizations worldwide do not fully measure recovery of business operations occurred in a timely fashion and in accordance with their disaster recovery plan

Ransomware has become a highly-publicized threat and a major risk to many individuals and organizations worldwide. It is a very destructive variant of malicious malware. When it infiltrates the network, critical systems and sensitive information become inaccessible until a ransom is paid. The ransom amount is typically paid via Bitcoins within 72 hours and if unpaid the key to unlocking data is deleted, making it almost impossible to recover. Those refusing to pay can face a permanent loss of systems and access to sensitive information, significant operational downtime, financial losses or liability and reputational damage.

With Ransomware causing major havoc in the past year, it’s alarming that so many organizations are uncertain they have backed up information properly and if they can recover it in a timely manner. Nearly two out of three businesses (64%) fail to recover timely and aligned with the disaster recovery plan.

In addition, a staggering 78 percent of companies do not fully or regularly test and measure their business continuity and recovery plans in order to learn whether they can recover from a business disruption.

Only 3 choices when you get hijacked by Ransomware:

1. Restore Backup or 2. Pay Ransom or 3. Do Nothing and Hope to Recover

There is a slim hope that law enforcement and the cyber security community may be able to capture and find the command and control servers and make the keys available to recover data. This, however, is a rare scenario and should not be relied upon. The best option to prevent Ransomware, is to ensure your Disaster Recovery plan is effective, prepared, planned
and tested. With 64% of organizations worldwide lacking a proven DR plan, there remains significant exposure by global enterprises to increasingly clever criminals and hacker threats.

75% of companies have not fully interpreted the regulations that apply to them, how to implement and measure compliance

CYBERSECURITY = COMPLIANCE?

Along with the growth in laws and regulations governing cybersecurity, many organizations globally appear to be taking a “checkbox” approach to security that focuses primarily on satisfying compliance audits. High profile breaches and subsequent fines for lack of proper security measures have spurred action to improve security postures. Thus, it is all the more shocking to discover that 75 percent of survey respondents have not taken adequate measures to ensure they are in fact fully compliant.

According to the 2017 Verizon Data Breach Investigations Report 81% of breaches used stolen/weak credentials

ACCESS TO PRIVILEGED ACCOUNTS A MAJOR VULNERABILITY

Access controls for privileged accounts in network systems are some of the most important ways to protect these “keys to the kingdom.” Privileged accounts include highly sensitive power accounts like those of a system administrator, or root accounts that if compromised can enable an attacker to move anywhere within the network undetected. Therefore, it is vital that organizations treat access control as a top priority for cybersecurity.

Yet, nearly two out of three or 60 percent of our survey respondents fail to adequately protect privileged administrator accounts.

60% of companies fail to have adequate security and processes in place to protect the keys of the kingdom, those sensitive Administrator Accounts

It is perhaps even more shocking that almost 70% of companies do not even know how many privileged accounts they have in their environment. Undiscovered or unknown privileged accounts mean organizations don’t know where they are
located, or who has access to them. Most organizations are shocked to discover how many privileged accounts exist in their environment and it’s not unusual to have 2-5 times the number of privileged accounts as users.

70% of companies have no idea how many Privileged Accounts they have!

Unfortunately, it appears that up to 70 percent of organizations have still not fully implemented a Privileged Account Management solution that should include automating the discovery of privileged accounts, storing passwords in a secure vault, rotating passwords on a regular basis, and monitoring access to privileged accounts.

70% still have not fully implemented a Privileged Account Management solution

We do however see progress as more companies are using Privileged Account vaults to store and protect credentials which is up from 10 percent from another survey report that specifically measured the State of Privileged Account Management. But with 70% of companies not fully implementing a comprehensive Privileged Account Management solution, we face a yawning gap in protecting the “keys to the kingdom.”

SECTION 3 - CYBERSECURITY METRICS NOT A PRIORITY

The main reason why the application cybersecurity metrics often falls short, stems from a lack of resources, according to survey respondents.

Question: Our security metrics are not contributing enough value because: The major reasons for why security metrics are not contributing enough value to the businesses in our survey included many of the usual suspects in terms of limited time and money.

We don’t have the time - 37.1%
We don’t have adequate resources - 42.7%
We don’t have sufficient knowledge - 28.4%
We aren’t allocating enough budget - 32.3%
Not applicable - 31.5%
*respondents were allowed
1. We do not have adequate resources  
2. We do not have enough time  
3. We do not have sufficient knowledge  
4. We do not have enough budget  

Given these constraints, cyber security solutions need to automate processes and simplify the management required to deploy and maintain. Complex, manual, labor-intensive cybersecurity solutions can not only impede productivity but can actually increase risks to the organization if they are not embraced by the staff that must use them on a regular basis.  

The lack of budget for security metrics may reflect a failure to communicate the urgency and importance of cybersecurity accountability among business and IT users, and a lack of buy-in from the executive management team.  

SECTION 4 - SMALL BUSINESSES ESPECIALLY VULNERABLE  

Small and mid-sized businesses are hit by 62 percent of all cyber-attacks, about 4,000 per day, according to IBM  

CISO’s, CIO’s and other executives are being measured by how well the business is growing, and ensuring that data used to make vital decisions must be accurate and validated. Any decisions made on compromised data can be devastating for any business. Small and medium size businesses (SMBs) are being targeted more because their cyber security is typically much easier to compromise. Though they are not usually the main target but a secondary victim, the real goal of cyber criminals is to infiltrate partnerships SMBs have established with larger organizations via a supply chain or data shared with larger companies.  

“60 percent of small businesses go out of business six months after a cyberattack”  
- U.S. National Cyber Security Alliance  

SECTION 5 - RECOMMENDATIONS TO IMPROVE SECURITY METRICS  

Results of the survey clearly indicate that cyber security metrics must become much more of a priority than they have been in the past. It appears that many organizations are making security decisions blindly without clear measurements about the impact on their cyber security posture, protect sensitive data, and ensure the business can recover efficiently from a breach. Most of all, enterprises must improve their efforts to collaborate with their business users to effectively secure their operations. Following are several recommendations based on the results of the survey.
EDUCATE ALL STAKEHOLDERS

Educate Employees and Measure Cyber Hygiene

The weakest link in the security of most organizations is the human being. As more sophisticated social engineering and phishing attacks have emerged in the past few years, companies must consider expanding their IT security awareness programs beyond simple online tests or acknowledgements of policies. As personal mobile devices are increasingly used for business purposes, educating employees on secure behaviours has become imperative.

All employees should be educated and made aware of cyber security threats. They should be trained and guided by best practices: becoming informed and aware of corporate security policies; how to choose strong and easily remember passwords; limit their activities using public Wi-Fi; use secure websites; and most of all “think before they click.” Cyber hygiene should be an ongoing learning process for all employees. Finally, enterprises must continuously measure the success and progress of cyber hygiene to identify gaps and focus on areas for improvements.

Mandate that C-Level execs experience a Red Team assessment

The enterprise’s executive team must lead by example. One way to get them involved is to conduct “Red Team” cyber exercise to vividly demonstrate how cyber threats occur and how quickly they can damage a company. A Red team exercise is a method using independent white hat hackers to test the effectiveness of an organization’s security defences and readiness to respond to a cyber-attack. This allows executives to experience what a real-world scenario is like, and how effective decision-making can avoid a disaster. It also helps educate top executives about cybersecurity risks and how to prioritize defences, including preparing an Incident Response team and plan to deal with any breach that may occur.

Implement an approach and culture of Least Privilege

It’s long past time for enterprises to start adopting a least privilege strategy when it comes to access to key data and admin-level network access. Privileges should only be granted when required and approved, eliminating the possibility of an attacker compromising your network by targeting privileged account passwords or hashes. IT departments must focus on enforcing least privilege access on end user workstations by keeping end users configured to a Standard User profile and automatically elevating their privilege to run only approved and trusted applications. For IT Admin privileged accounts, access to accounts must be controlled using Super User Privilege Management for Windows and UNIX systems to prevent attackers from running malicious applications, remote access tools and commands.

PROTECT CRITICAL SYSTEMS

Backup critical data and systems and customize your recovery plan for different types of cyber threats. Test your restore capabilities.

As the recent global ransomware attacks dramatically demonstrate, enterprises must institute an effective and efficient disaster recovery plan for all types of business risks. Business continuity is essential, yet many companies still do not tailor their disaster recovery plans for specific cyber threats. Many companies, for example, have restored a backup to recover from a malware infection only to find out their backup data was also infected. When evaluating the risk assessment for cyber threats, your disaster recovery plan should be modified to compensate for different types of cyber
threats including DDOS attacks, malware infections, data loss or corruption by ransomware.

**Ensure Multi-Factor Authentication is in place**

Multi-factor authentication is becoming standard practice these days, including authenticator applications (Google, Microsoft, Symantec, Authy, Duo) to SMS. It's important to enable alerts and notification on your accounts so you can be notified of any suspicious activity. Multi-factor authentication is a proven method for making the attacker/hacker’s job much more difficult to compromise an account. It also allows a company to establish a level of trust between the user and system, and challenge user access when any suspicious activity occurs.

**Strengthen Identity Access Management and Protect Privileged Accounts**

Fast growing technologies such as Cloud, Mobile, and Virtualization have transformed the boundaries of global organizations. For many years organizations have protected their valuable and sensitive information by building a perimeter fence around their assets. Data that flowed in and out of that organization was channelled either through a single internet access point or on physical devices. This traditional perimeter worked because the boundaries were known.

In today’s interconnected world organizations can no longer rely on the traditional security perimeter as their only cyber security measure. The new cyber security “perimeter” must incorporate Identity and Access Management of employees and third-parties. It reflects the new reality whereby systems and data can be located anywhere and be accessed at any time if the identity and access can be validated and trusted.

Only through an effective policy and best practices approach based on Identity and Access Management, will a company be able to accelerate new technology adoptions and at the same time protect itself from becoming the next victim of hackers or cyber-criminals.

**Prepare and Implement a Cyber Incident Plan**

When a security incident occurs (it’s no longer if but when) your company must be prepared to respond when you find out you have experienced a breach. In many cases you may not even discover the breach yourself but will informed of it via a third party such as law enforcement. Your response plan will determine how well and quickly you can limited damage from a breach, recover, and restore confidence with customers, shareholders, and partners. An effective incident response plan must include: how to deal with the incident; who needs to be involved and when; define the role of various stakeholders such as CEO, Legal, PR, Social Media, and IT Security; how to inform impacted customers; and ultimately how to recover and restore services.

**MONITOR AND CONTROL**

**Control, Monitor, and Report Admin Privileged Access to Systems**

Privileged accounts are the top target of any attacker because they provide access to sensitive data and enable the attacker to move anywhere within a network undetected. The typical route taken by an attacker begins by gaining a foothold in the
network by any means possible. That usually occurs by exploiting an end-user computer, then working to elevate access by compromising a privileged account, which enables the attacker to operate on a network as if they are a trusted IT administrator. Thus, it is extremely important to control and monitor the use of privileged accounts across the enterprise.

Controlling privileged access should be a top priority for all companies in 2017, helping to reduce privilege abuse from malicious insiders as well as making it much more difficult for external hackers to compromise these accounts.

**Correlate, Monitor and Audit Security Logs**

Far too many global organizations are still failing to collect essential security and audit logs especially when performing evidence gathering or digital forensics. This kind of data is vital to determine the “what, how and when” of incidents. Without this vital information, any root cause analysis must rely on assumptions that may not be accurate. Correlating and monitoring security and audit logs should become a standard routine, and will help a company reduce the impact from cyber-attacks by finding and eliminating security issues early, before they escalate.

**MEASURE**

**Get your Key Business Metrics Sorted**

At the moment, the difficulty measuring cyber security risk and effectiveness for many organizations has challenged the CISO in demonstrating how cybersecurity can show business value. The metrics are still evolving and for most cyber security professionals, it’s been about keeping the existing security controls working, make continuous improvements where possible, and placing security on previously adopted technologies. Cyber security has typically been an afterthought, making the CISO’s already tough job more challenging.

As cyber security continues to capture more attention at the boardroom level, measuring the planning and performance of cybersecurity investments will hopefully get more sophisticated and helpful. The stronger our metrics, the better our odds of making smart decisions that keep our businesses growing safely and securely.

**Take the Security Measurement Index Benchmark Survey**

Based on ISO 27000 international standards and input from security professionals, the Security Measurement Index gives you an easy to understand benchmarking tool for assessing how your organization’s security measurement practices compare to those at other companies.

Upon completing the online survey, you get:

- An immediate grade (A through F) rating how well you measure your IT security efforts based on best practices.
- A follow up email that includes a report on how your answers compare with your peers who have taken the survey.
APPENDIX A – METHODOLOGY

SECURITY MEASUREMENT INDEX BENCHMARK SURVEY SCORING METHODOLOGY

The Benchmark has a maximum of 164 points possible. Not every question is scored; for example, questions about your industry or number of employees do not carry any score. Questions about security measurement procedures and practices do carry a score value. The grade received at the end of the survey is based on the following scale.

147 to 164 points = A
131 to 146 points = B
114 to 130 points = C
98 to 113 points = D
0 to 97 points = F

Your Grade is an “A” if your score is between 147 and 164. Your organization is exhibiting numerous best practices related to measuring the effectiveness of your cybersecurity programs. You likely engage with your business users and have strong security policies in place, with sound procedures and technology to support your security posture.

Your Grade is a “B” if your score is between 131 and 146. Your organization is meeting many best practices related to measuring the planning and performance metrics for cybersecurity, but could improve some of your processes and metrics. Your comparative answers follow up report will help you determine key areas for improvement.

Your Grade is a “C” if your score is between 114 and 130. Your organization is “average” when it comes to planning and implementing cybersecurity metrics. While you may have a policy and some general best practices in place, you should focus on more rigorous procedures for measuring whether practices are properly followed.

Your Grade is a “D” if your score is between 98 and 113. Your organization is missing several best practices regarding cybersecurity metrics throughout your network environment. You are likely in a position where you must first achieve better fundamentals in terms of identifying sensitive information, where it resides, and how it moves through your network. Only then can you begin to measure your cybersecurity effectiveness.

Your Grade is an “F” if your score is between 0 and 97. Your organization is not meeting most best practices regarding cybersecurity planning and performance metrics. This may expose your organization to significant security vulnerabilities and compliance deficiencies if not addressed soon. Ensure you have a strong policy, look for admin and other privileged accounts in use within the environment, and ensure management understands that measuring cybersecurity needs to be a top priority for you.

SURVEY DEMOGRAPHICS

The majority of the more than 400 survey respondents came from North America, with Europe, Russia, India, Central and South America also represented. The global response featured all major industries including financial, technology, manufacturing, healthcare, government and more. Survey respondents represented a cross section of global organizations...
ranging from small and mid-sized companies to large global enterprises.

Both high profile breaches and cyber terrorism have likely raised the awareness of threats to businesses as the possibility of a catastrophic event can apparently reach anyone, anywhere in the world. This is reinforced by the recent global ransomware attack that affected 200,000 Windows computers in more than 150 countries, including China, Japan, South Korea, Germany and Britain. Cybersecurity as a major, integrated business priority is here to stay. The better we are able to measure its effectiveness, the sooner we can our businesses safer and more secure.

APPENDIX B – FREE RESOURCES

FREE LEARNING TOOLS

Free Privileged Password Security Online Training ensures you and your staff are up-to-speed on the importance of privileged account security and best practices to protect passwords.

FREE SECURITY TOOLS

Free Weak Password Finder for Windows Tool gives you an immediate and easy way to Identify where the weak passwords are located across your organization.

Free Privileged Account Discovery for Windows Tool enables you to find privileged accounts across your enterprise, including many that are unknown and unmanaged.

Free Windows Endpoint Application Discovery Tool saves you hours of effort by discovering vulnerable applications and their associated risks in minutes.

Free Security Policy Template for Privileged Passwords saves hours of time and effort with easy-to-customize templates that help you improve security and meet compliance mandates.

FREE BENCHMARKING TOOLS

Free Password Vulnerability Benchmark lets you see how your password protection efforts compare with those of your peers.

Free Security Measurement Index lets you see how your security measurement efforts compare to those of your peers.

ABOUT THYOCOTIC

Thycotic prevents cyberattacks by securing passwords, protecting endpoints and controlling application access. Thycotic is one of the world’s fastest growing IT security companies because we provide customers with the freedom to choose cloud or on premise software solutions that are the easiest to implement and use in the industry. Thycotic has grown to serve more than 7,500 customers. To learn more, visit www.thycotic.com