Check Point®
SOFTWARE TECHNOLOGIES LTD

WHY COMPLIANCE MATTERS

WE
SECURE
THE
FUTURE

TABLE OF CONTENTS

WHY COMPLIANCE MATTERS

INTRODUCTION

Compliance is time consuming, complex, and often appears disconnected from our "real" work. It is not surprising that we often find ourselves asking, does compliance matter anyway? The truth is that today, no matter what your role, compliance is becoming more significant to our businesses than ever before.

Today security and compliance teams are faced with a plethora of security standards and regulatory obligations. While standards typically provide recommended guidance, regulations are mandatory and must be addressed. Non-compliance can lead to fines and penalties, and even worse, potential damage to the organization's reputation. For these reasons and more, compliance does indeed matter. But why develop regulations anyway? If individual organizations are left alone to determine appropriate levels of security, this leads to dramatic variation in security from organization to organization. Potentially, this leaves those organizations, and anyone who works with them, more vulnerable.

The creation of standards and regulatory requirements leverages the knowledge and expertise of the greater security industry to provide a common security baseline.

Implementing this baseline across organizations enables standardization and uniformity within the organization, and promotes accountability among both organizations and individuals.

Further, today compliance means more than meeting the requirements of a one-time or periodic audit. The compliance environment has evolved to require organizations to demonstrate ongoing attainment of the minimum standard of performance. Doing this manually would be an impossible task. Continuous compliance monitoring enables organizations to know what is going on across the network in near-real time, and ensure alignment with required regulations.

Continuous compliance matters not because of standards, but because our businesses are in a constant state of flux. If we want to increase our chances of preventing security exposures, we must embrace compliance and embed it into our business practices.

STANDARDS AND REGULATIONS

The Merriam-Webster1 dictionary defines the word compliance as "the process of complying with a "proposal" or "conformity in fulfilling official requirements".

These two definitions perfectly summarize the world of compliance today. On the one hand, standards abound, including position papers and best practices helping and informing business how to behave and act. The United States is particularly active in this regard. A quick review of NIST guidelines, the National Institute of Standards and Technology, reveals hundreds of guidelines ranging from secure configurations of Internet Explorer, all the way to the Google Android platform.

On the other hand, countless regulations force companies to behave in a particular way. Usually this is driven by a national agenda, such as privacy, which is then in turn translated into a proliferation of specific privacy acts, each country's law being slightly different. Another example would be corporate financial health—large corporates are the lifeblood of most economies, generating employment and taxes. Should these businesses fail (the banking industry being of particular concern) this can have a devastating impact on a local economy—hence government intervention resulting in laws such as Sarbanes-Oxley and its variants around the world.

There is often an overlap between standards and regulations. FISMA, the Federal Information Security Management Act, a mandatory act by law, requires companies to comply with FIPS 200 which in turn makes a reference to NIST 800-53: Recommended Security Controls. What was once just a guideline was eventually "upgraded" to a full regulation. Whether compliance is voluntary or mandatory, the commonality spanning these two concepts is that we ourselves do not know enough to, or cannot be trusted to, manage our own corporate affairs.

Whilst this may seem unfair, the large number of scandals, both minor and major, testifies to this reality.

The KT Corporation, in South Korea was hacked in 2012 when two men allegedly stole user information from more than 8 million KT mobile phone subscribers. The hackers sold the data to various marketing companies, which reportedly used the information to solicit subscribers and convince them to switch service providers.

THE WISDOM OF CROWDS

The Wisdom of Crowds, written by James Surowiecki, gives us the idea that the total knowledge of the group will be superior to the knowledge of the individual. Take the success stories of Wikipedia, or of Waze, and countless other examples, to explore how "communal" knowledge is generally better than "personal" knowledge.

This concept is embedded in compliance. Why struggle to determine how to secure your latest hardware or software purchase, when there are guidelines and standards that have been written and approved by a vastly knowledgeable community? If you haven't done it countless times before, why attempt to harden your new server when many people done it already and their wisdom has been pooled and made available to you, often free of charge.

This idea is very powerful and yields many advantages. First, it achieves standardization and uniformity. By using pre-defined baseline configurations, companies are able to define standards for themselves and request that all offices adopt them. This does require a degree of abrogation of personal power (on the part of the satellite offices) to a central authority but in general it is better for the manager to know that everything is being managed in the same way.

Second, it achieves accountability and responsibility. The corporate center has defined what is secure and what is not secure. Here we have achieved corporate authority. By requesting that these standards are implemented throughout a company, individual security personnel are then responsible for their execution.

Once this is in place, it allows for exception management policies to be instituted and derivations from the secure baseline to be monitored and approved as needed. This model generates and supports personal accountability and responsibility, a cornerstone of all security programs.

Third, it allows portability. Portability means the ability to move between companies and re-use knowledge gained from one in the other. It ultimately allows the shifting of human resources to be trained and to develop detailed knowledge that is transferable. This allows companies to hire staff with the requisite skill sets needed to take on postions and responsibility.

MONEY AND REPUTATION

While the wisdom of crowds helps to explain guidelines and best practices, it doesn't justify the growth of security-based regulations. Yet this growth is based on precisely the same principle—uniformity. Governments, or in the case of PCI-DSS, the credit card industry itself, seek to ensure consistency to ensure a minimum security baseline. This guarantees a level playing field for those operating in the corporate sector.

The implementation of standards drives uniformity and consistency on a macro level. On the micro level, businesses also define centralized policies and demand that they be implemented across the company. The significant difference though between government and business is the ability to enforce. A regulation is only as strong as the issuing authority's ability to monitor, track, and enforce, and of course to punish as needed.

Security incidents cost money. One report on the UK business sector highlights that the average cost of a large organization's worst security incident is £450,000 to £850,000. The average cost of a small business' worst security incident is £35,000 to £65,000. "In total, the cost to UK plc of security breaches is on the order of billions of pounds per annum—it's roughly tripled over the last year."

Yet the reality is that all these companies can afford these financial penalties.

Security incidents also result in regulatory fines. From large events such as Sony being fined £250,000 for its "preventable" PSN hack or Blue Cross Blue Shield of Tennessee agreeing to pay $1,500,000 to resolve violations of the HIPAA Privacy and Security rules, down to smaller events such as The Hospice of North Idaho paying $50,000 for security breaches. Financial penalties are painful and are still a large motivating factor for many a network security or compliance manager. No one wants to be responsible for causing the company a significant financial loss.

So if this is the case, then what is the real driver and motivation? In short, it is reputation. A fine can always be paid—gone and forgotten. A stain on one's reputation lasts a long time. In a climate where the consumer is savvy enough to know that there are always other options, customers do not share the same commitment to a brand or business that they once did. Embarrassing incidents lead to customers leaving, to brand erosion and to a reduction in long-term value, and therefore much more severe in terms of loss than a fine.

CONTINUOUS MONITORING

Perhaps one of the most important shifts in the compliance "industry" has been the transformation of periodic auditing to continuous monitoring.

Traditionally, the role of audit has been akin to a "spot check"—a team of people, be they internal auditors, or an external third party, come to a specific business operation, perform a review, document the findings, and submit a report. Based on the findings, there may or may not be follow up items. The business has time to implement the findings as needed. And then life goes on as normal, until the next audit. This audit mechanism has proven to be very powerful.

Audits are mandated by the executive layer of the business. The audit is the executive's best chance and ensuring that things are being run properly and is therefore a critical tool for them to flag small issues before they become big issues. The power vested in the audit department ensures that it can't be messed with and it will do its job properly.

The construction of the annual audit plan allows the business to insert a degree of randomness which in turn generates spontaneity. While an audit is never truly random as they are always communicated in the past, knowing that someone is coming to check you when they are ready, and not necessarily when you are ready, is a sobering thought. The audit plan also means that "it could be you"— meaning, we need to keep constant vigilance in our business practices because at any time it could be us that becomes the subject of the next audit. Any operation that goes unchecked has the potential to spiral out of control.

Furthermore, the auditors' professionalism empowers the team to ask the right questions in the right places. For this reason, auditors undergo training to ensure they understand the scope and subject of their audits. If during an audit the operation knows how and where to hide things, they are unlikely to be uncovered. If however the auditor understands the operation very well, they have a stronger chance of revealing what was not meant to be found.

So if traditional audit approaches work, why the shift to continuous monitoring? Whether we like it or not, this is the direction of security monitoring. In the NIST 800-53: Recommended Security Controls document, it states that "the organization establishes a continuous monitoring strategy and implements a continuous monitoring program."

Regulation	Reference	Requirement
NIST 800-53: Recommended Security Controls	CA-7	" The organization establishes a continuous monitoring strategy and implements a continuous monitoring program"
Critical Controls for Effective Cyber Defense—SANS Institute and NSA	Page 4, Step 4	" Integrate Controls into Operations—focusing on continuous monitoring and mitigation"
NIST 800-137: Information Security Continuous Monitoring	Whole Document	" Ongoing monitoring is a critical part of that risk management process"
NIST 800-37: Risk Management Framework	Page 10	" Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes"
Technology Risk Management Guidelines —Monetary Authority of Singapore	4.5.1	" A monitoring and review process should also be instituted for continuous assessment and treatment of risks."
NIST Guidance on HIPAA	164.308(a)(8) 164.308(a)(1)(ii)(D)	" Monitor and assess selected security controls in the information system on a continuous basis"
PCI DSS	11	" System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment."

Figure 2: Regulations Referencing Continuous Monitoring

And though it may appear that continuous monitoring is the sole endeavor of the United States, it is also visible across Europe and Asia. Financial Executives International published research showing a major trend across 14 of Europe's largest public companies that … "almost without exception, European companies are either moving toward or least seriously considering the introduction of some form of Continuous Control Monitoring." And in Singapore, the local government's Technology Risk Management Framework states that "A monitoring and review process should also be instituted for continuous assessment and treatment of risks."

While traditional audit approaches do work in general, in the world of Technology, the rate of change of the IT environment is far too quick to allow a year to go by without rechecking the situation.

And often it was more than a year, sometimes up to three years. Today, there is a growing expectation to understand what is happening between the audits, not just on the date of the audit. If a significant event or breach were to happen, it wouldn't be acceptable to claim that the controls were checked six months ago.

This is one of the ironies in Information Security—on the one hand we have the ISO27001 standard that is perhaps the most prolific security framework worldwide. Yet on the other hand, businesses clamber to have an ISO certificate hanging on their wall (or website) that testifies to a period of time long gone, with a limited scope, with a list of open action items to be implemented over the coming years.

ISO27001 certainly has its place, and its Plan-Do-Check-Act model of continuous improvement is one that all should adopt. However there is a difference between what the authors wished to achieve, and the oft-mentioned "just get me certified" approach of many companies.

Technology has improved significantly and has enabled businesses to check things with a much greater frequency than was previously possible. This suggests that traditional auditing would have adopted continuous monitoring much earlier had it been available or feasible to implement.

COMPLIANCE AND SECURITY

There are calls today on governmental bodies to lower the oversight burden. it is time consuming, inefficient, and occupies our resources. In a perfect world, where companies and individuals operate perfectly, one could imagine a scenario where regulations and standards are actually cancelled and removed from our day to day activities. Yet we aren't living in a perfect world. Companies are facing rising cybercrime, targeted hacking is getting worse, and we are seeing more and more instances of state-sponsored cyber terrorism. On the personnel level, employees face an onslaught of new technology, uncertainty how to use it, and poor communication of simple security policies, leaving us extremely exposed.

Compliance matters because regulations and standards are the best hope we have to standardize security practices and increase our capacity to protect ourselves from cyber security threats. One should be wise to look forward to the future and see how integrating compliance into day to day activities can be achieved because it's here to stay, and its role in day to day security will only increase.

CHECK POINT COMPLIANCE MANAGEMENT

Check Point's Compliance Management leverages decades of security expertise and extensive knowledge of regulatory compliance, providing a holistic view of the security and compliance status across Check Point Gateways and Network Security Software. With the Compliance Management, network administrators can easily identify potential security breaches and vulnerabilities and receive practical guidelines on how to remediate security weaknesses.

COMPLIANCE MANAGEMENT OFFERS THE FOLLOWING KEY BENEFITS:

- *Security monitoring across Check Point Software*
- *Real-time assessment of compliance with major regulations*
- *Instant notification on policy changes impacting compliance*
- *Actionable recommendations to improve security and compliance*
- *Automated assessment reporting*

Check Point's Compliance Management is perfectly suited to every company no matter their size, industry or location. Since the product not only assesses compliance to regulation but also provides recommendations on best practices, it is relevant for companies that operate in both a high or low regulatory environment.

REFERENCES

1 http://www.merriam-webster.com/dictionary/compliance

2 http://www.databreachtoday.asia/korean-hack-affects-8-million-a-4996

3 https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

4 There are many research articles that support this theory. See for example Check Point's 2013 Security Report (http://www.checkpoint.com/campaigns/security-report/index.html) or James A Lewis' report on "Raising the Bar for Cybersecurity (http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf).

5 https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

6 http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

7 The Wisdom of Crowds was published by Random House in 2005 (http://www.randomhouse.com/features/wisdomofcrowds)

8 Wikipedia was launched in 2001 by Jimmy Wales and Larry Sanger. Their departure from expert-driven encyclopedia writing towards a collaborative model was challenged by the Encyclopedia Britannica. In 2006, a study performed by Nature determined that the error rate of Wikipedia was no different to the error rate of mainstream encyclopedias (http://en.wikipedia.org/wiki/Wikipedia)

9 Waze is the world's fastest-growing community-based traffic and navigation application (http://www.waze.com)

10 PCI-DSS is the Payment Card Industry Data Security Standard which provides an actionable framework for developing a robust payment card data security process (https://www.pcisecuritystandards.org/security_standards/index.php)

11 https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report

12 http://www.guardian.co.uk/technology/2013/jan/24/sony-fined-over-playstation-hack

13 http://www.hhs.gov/news/press/2012pres/03/20120313a.html

14 http://www.hhs.gov/news/press/2013pres/01/20130102a.html

15 http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

16 http://www.sans.org/critical-security-controls/

17 http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

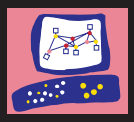
18 http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

19 http://www.oversightsystems.com/blog/?p=949

20 http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Technology-Risk.aspx

21 The objective here is not to slur ISO27001 as a standard—as stated this is a widely used baseline and is operational all over the globe. However one must consider the reality that many businesses want a certificate on the wall to attract or retain customers and therefore abuse the ISO process to achieve that. Note that it is always worthwhile requesting the scope of the ISO certificate to determine what was reviewed and what was not. Often the scope of the certification ismuch smaller than the casual observer would have realized.

22 A cursory search on Google will provide countless articles on the rise of cybercrime. See for example http://www8.hp.com/us/en/hp-news/press-release.html?id=1303754, or http://www.business-standard.com/article/technology/ibm-study-warns-of-rising-cyber-crime-112121400625_1.html



Check Point®
SOFTWARE TECHNOLOGIES LTD

WE SECURE THE FUTURE

To learn more about Check Point's Solutions for Security Management,
please visit www.checkpoint.com.com/management

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

March 2016