Communication and Collaboration: Essential Ingredients in Compliance

Redbooth Private Cloud
The Behind-the-Firewall Collaboration and Project Management Solution
# Table of Contents

I  Introduction: The Pillars Are Necessary, But Not Sufficient ....................................................... 3

II  When Secrets Are Incompatible With Security .............................................................................. 4

III  Silos and Tunnel Vision: How Jargon and Implicit Knowledge Create Challenges............ 7

IV  Why “The Binder” Won’t Be Enough: Becoming Audit-Ready .................................................. 9

V  Expecting the Unexpected: From Turnover to Catastrophes ................................................... 11

VI  Partial Solutions: Meetings, Emails, and Trainings ................................................................. 12

VII A Collaborative Future: Steps You Can Take ............................................................................ 13
When most people think of necessary ingredients in security compliance, communication and collaboration are not at the top of the list. Here, we look at how a paradigm shift is necessary in many organizations — from silos to engagement, from isolation to buy-in and engagement from stakeholders at every level.

I. Introduction: The Pillars Are Necessary, But Not Sufficient

Few things are more challenging than to protect a company’s data from external and internal threats. It’s not for lack of guidelines, though. A great deal of time, energy, and brain power has gone into developing security programs in the last few decades.

At one end of the spectrum is the library of guidance from the federal government’s National Institute for Standards and Technology (NIST), which has produced standards like Special Publication 800-53, a benchmark for cyber security and a technical security catalog of controls.

NIST SP 800-53 is an impressive work, with 17 families of controls — and within each one, dozens of individual controls. It is an encyclopedia of technical, administrative and managerial controls, but it is intimidating for even veteran security professionals.

Slightly less weighty is the Payment Card Industry’s Data Security Standard (PCI DSS), with only 12 “requirements” and associated controls. It seems to have boiled down an impressive number of security requirements into only 100 pages or so.

Most security and compliance professionals will admit that there is a lot of overlap in security guidance. There are some “pillars” of strong security, such as strong authentication, or best-practices such as backup and recovery, incident response and encryption.

Both sets of guidelines include some standard methodology: risk assessment, determining priorities, protecting and designing
controls to mitigate risk, setting up monitoring to ensure that controls stay in place, and starting the process all over again. It’s a rotating cycle of risk assessment, control, and maintenance.

These regulatory guidelines are valuable in defining the “what” of security. What they don’t talk about is the “how” — how you’re actually supposed to design your security program. It’s often necessary to bring in security consultants because the guidelines do not supply enough practicum.

In many ways, the rules are not sufficient. So even if you follow them to the letter, they don’t guarantee that you’re secure. Every company creates their safeguards and security protocols a little bit differently. And in the process of focusing on these guidelines, many companies overlook key elements that will be necessary for both compliance and security.

In this report, you’ll see why collaboration and communication in particular are commonly forgotten when it comes to developing, refining, and implementing security practices, and how deliberately and thoughtfully bringing them into the picture can help make your organization more compliant and more secure.

**SUMMARY**

- Federal guidelines for compliance are detailed but not necessarily helpful in planning implementation
- When mapping out a security plan, consider the importance of building in collaboration and communication

**II. When Secrets Are Incompatible With Security**

At first glance, the idea of collaboration might seem out of place in the security realm. Surely, the gold standard would be more about keeping information protected than encouraging an exchange of information.
Culturally, there can be a bias in some organizations toward secrecy, dating back to the days of “loose lips sink ships” posters on the walls of national government agencies.

On the surface, this approach might seem to make the most sense. However, what complicates things is that often important security information must be understood and utilized in a constantly changing and imperfect system. In such a system, being able to communicate about this information is essential.

Imagine buying a new house. Should you lock the door and keep the key with you when you go out? Yes, of course. But after a few weeks, complications start to arise. You want to give your next-door neighbor a key in case there’s an emergency. The cat-sitter needs a way to get in when your flight home from a trip gets delayed. You’re mowing the lawn — can you just leave the door open while you do it?

Start to add in other twists: the lock is actually a little tricky and you have to know how to get it to work, there’s an alarm code that you change every few weeks, the cat-sitter gets injured, can’t make it up the front stairs anymore and sends a substitute. The complications multiply rapidly.

What should be a simple issue of securing your home becomes more complex because you have to share access and depend on other people, each of whom is dealing with an array of ever-changing variables as well.

Surely the answer can’t be to make keys for everyone in the neighborhood or to put the alarm code on a post-it on the front door. But not sharing the right information with key people at key moments can also create new and significant risks, challenges, and vulnerabilities.

A common security incident illustrates this concept. After sensitive information is leaked in an organization, sometimes the leak can be traced back to a single person who told someone else about a risk or vulnerability in a bar or other public setting. The wrong person overheard and took advantage.
When the speaker is finally identified, it may be someone actually who was cleared to have that piece of information. However, when the information was conveyed, it didn’t come with a clear warning that it was confidential.

Because of situations like this, organizations sometimes find that they need more communication around the transmission of information. The key to greater security in this case is more communication, not less.

There can be a tendency for the pendulum to swing all the way to one side, shifting to a different approach that feels secure on the surface: “Don’t write things down on paper or digitally,” some people say. “Just have a private conversation.”

At least this way, the thinking goes, there will be no records to be found or hacked into. But verbal communications are as prone to problems as written communications, and in some way, more so. And in many cases, secure written systems offer additional safeguards.

For example, in a written system, you can build in routines to remind users that the communication that’s about to occur or the information they’re about to access is sensitive. They’re then more likely to treat it accordingly.

Additionally, people do forget things. This is compounded by the fact that they’re often dealing with more security-related issues — and certainly more information in general — than in the past. With hundreds of emails and dozens of projects to keep track of, processing and especially retaining information is more challenging than it used to be.

It is, in large part, because people are fallible and forgetful that many security protocols are needed. But for those same reasons, it’s essential that practices exist in a way that accommodate the forgetfulness and fallibility as well.
SUMMARY

- It’s important to make a distinction between a culture of security and a culture of secrets, since secrets can get in the way of actual security.
- Real-life complications mean that it’s essential to consider context in crafting and implementing procedures.
- Processes that may seem intuitively secure, like discussing something in person instead of communicating it in writing, come with their own unique risks that need to be managed.

III. Silos and Tunnel Vision: How Jargon and Implicit Knowledge Create Challenges

The threats faced by security professionals have morphed to an extent that might have been nearly unimaginable a few decades ago. In the 1980s, slow computer systems and slow (if any) networks required a simpler approach to security. Passwords were simpler, and most people were not as worried about risk when computers were only running one program at a time. The “lock on the door” method was actually enough in many cases.

Since those days, the very concept of what security consists of has evolved dramatically. Of course, the security challenges organizations face today are not going to be satisfactorily addressed by putting a lock on the office door. Information can leak from a rapidly increasing number of sources and devices, and once shared it can spread like wildfire.

In some cases, though, remnants of the lock-on-the-door culture can still be found in modern organizations when it comes to security. Sometimes the department responsible for computer security is itself siloed, with the knowledge around risks and protocols restricted (explicitly or tacitly) to the experts.
There’s a continued gap between the people who have information about how to secure systems and data, and the people who control those assets. How do you get closer and closer to closing that gap, if not through communication?

Listening to stories about computer hacking, you will commonly find that it was not actually a security tool that triggered the warning of “Hey, someone’s hacking in.” Instead, it was someone looking at the logs and seeing a pattern — noticing small details that seem out of place and putting the pieces together.

This mosaic effect is remarkable — and it depends on the people who are in a position to notice being empowered to stay alert and to share what they notice. Fundamentally, it depends on a dynamic communications system where protection and assessment measures are commensurate with the risk to assets and communicated rapidly to business and operational teams.

In actuality, this is not a challenge with a single origin. Everyone has tunnel vision, and that includes employees inside and outside of the security realm. It’s helpful to make sure that the security professionals within an organization are accessible — speaking to people more, sharing more, and in language that people understand.

People in the organization who don’t think they need to worry about security may have access to very sensitive information. In some ways, they are among the most important stakeholders to engage. Unfortunately, they’re not always receptive — but it’s important to be resourceful in finding ways to engage with them nonetheless.

**SUMMARY**

- We know that a simple “lock on the door” mentality doesn’t work anymore, but this once-effective mindset can still be found in other forms within organizations.
- Overcoming the department silo effect is essential, because everyone who has access to sensitive information needs to understand the immediate and far-reaching impacts of their actions

IV. Why “The Binder” Won’t Be Enough: Becoming Audit-Ready

We’ve all seen “the binder” that sits on a filing cabinet, full of procedures and configuration information — and rarely opened. While the procedures in that binder might be an excellent start to documenting and thinking through security protocols, the binder itself poses a hidden danger: its existence can give an organization a false sense of audit-readiness and security.

That’s because it’s people that make those security protocols work. For example, encryption involves key managers, sophisticated procedures, the ability to issue keys and revoke keys — all of that doesn’t just happen automatically as a result of somebody writing a out a procedure. It’s critical to collaborate on procedures and to be able to ask questions about things that aren’t written perfectly the first time around.

Even when a procedure is written clearly and easy to locate, there will still be questions. Where, exactly, is the backup tape safe? We’re using a third-party outsourcer — what’s their phone number? It’s crucial to ensure that your written security procedures are questioned and understood by people in your organization.

In an audit, often auditors are not just going to check on written procedures and speak with the CIO. They may go in and talk to staff: Do you actually know how to do the backup? What would you do if you had to do a recovery? And what’s your backup for the backup? Respondents need to have a living knowledge of the procedures in a dynamic context, not merely academic knowledge of the procedures as written.
Auditors observe and conduct interviews. They test the data and they test the means by which data is collected or processed. This could mean interviewing a network admin, or a processing clerk, or people who are interacting with the system of record.

A common audit plan would include doing a number of tests across a variety of different areas to prove that (a) what is stated is true, and (b) that the people who actually have to enter that information understand what it actually means.

And when the processing clerk has all the right answers, the auditors are also going to ask: What happens if that clerk is gone? It’s about both the veracity of the information and the tenacity of the organization.

And every year, the bar just keeps rising. Risk levels increase, opportunities for data leakage increase, and people who would like to breach your security get smarter and more resourceful. Revisiting written procedures in a binder or a file on an annual basis is simply not going to give you the results you need.

Audit programs like FFIEC, GLBA, HIPAA, and PCI do not lower standards over time — they raise them. Likewise, audit programs and auditors are becoming more sophisticated in their methods and practices. Don’t bank on a compliant program remaining so without staying up to date with risks and technology changes occurring all the time.

**SUMMARY**

- Static procedures may work perfectly on paper, but without taking into account the questions and challenges of the people who will implement them, they may not offer sufficient protection
- Preparing for an audit requires an ever-increasing level of organizational preparation, including ensuring that individuals at every level understand and can implement procedures
V. Expecting the Unexpected: From Turnover to Catastrophes

Security is largely about expecting and preparing for the unexpected. If you follow the news, you know that high-impact, low-frequency events are headline material, such as when a utility transformer gets blown up by a hacker, a large, well known business attack causes severe damage, or a natural disaster hits. A catastrophe can be spectacularly damaging to a business. At the same time, we recognize those events are still fairly uncommon.

Meanwhile, another potential threat to compliance and security is happening much more frequently: employee turnover. It’s the reality of the marketplace that many people, including those in technical and security-related fields, will change jobs frequently. If you’ve just trained somebody on a specific skill that is required and that person walks out door, you’re out of luck when an auditor walks in or there’s an incident — because you don’t have someone on hand to illustrate that a critical security program is operational. Meanwhile, the new person hired for that role doesn’t know how to immediately access the procedures and the tacit knowledge surrounding them. It’s not a change anywhere on the scale of a disaster, but the results can be problematic — leading to security incidents, findings, and fines.

A lot of businesses resist thinking about the unthinkable, or rely on reassuring-sounding systems without delving deeper. It’s preparation, entertaining uncomfortable possibilities, and asking hard questions that will help make it possible for an organization to weather a catastrophe.

So how can this be achieved? Dialogue within an organization can help. Discuss how to mitigate potential damage and how to disperse your assets. If you do have a binder full of procedures, start by moving the business continuity and disaster recovery plans from the back of the binder to the front. Talk to technology
vendors about disaster readiness before you sign a contract with them. Don’t get complacent, and just as importantly, don’t let the decision-makers in your organization become complacent either.

Creating working groups within organizations or industry-wide can also make a difference. The disasters and tragedies of recent decades functioned as a wake-up call for many in regard to preparing for and protecting companies and their assets.

**SUMMARY**

- We don’t like to think about the unthinkable, but preparing for a variety of potential disasters is a crucial part of protecting the assets of your business
- Everyday challenges also require planning and preparation, including simple employee turnover

**VI. Partial Solutions: Meetings, Emails, and Trainings**

Handouts. Company-wide emails. Software upgrades. A half-day mandatory training. These are all partial solutions: helpful, but usually not enough. Like a binder full of security procedures, they can provide a false sense of security: “We did a training, so we’re set for a week, a month, a year.”

But threats are ongoing, and you’re going to need an ongoing assessment that extends throughout the organization continuously. What are the risks today, and what information do we have to inform us of what that change in risk profile is? Even with advances that may seem like panaceas to some, like biometrics, the truth is that security will continue to permeate everything that touches technology and touches value. You can’t just do one training or occasional upgrades. It takes a cultural change.

And almost everyone now agrees that one big training a year
will not change the culture of a company. Meanwhile, that culture is morphing and evolving on its own, not always in lower-risk directions. As organizations hire increasing numbers of millennials, for instance, their workforce is increasingly full of employees who grew up with screens and have very different ideas about technology, privacy and disclosure.

In the final section, we will look at what you can do to gradually change the culture of security within your organization — and to move toward making security practices something that exist dynamically in a system where they can be questioned, accessed, understood, and implemented in a way that is compatible with growth and change.

**SUMMARY**

- Be careful not to put too much weight on one-step responses like trainings or company-wide announcements; while useful, they are rarely complete solutions
- Be prepared for waves of internal culture change resulting from a workforce’s changing demographics and approach to technology and privacy

**VII. A Collaborative Future: Steps You Can Take**

So what kind of foundation can you put in place to be prepared for everything from an audit to a potential breach? There are a variety of practices that can be helpful:

Maintain a virtual space where dialogue can take place securely and questions can be asked and answered — and contribute to a culture of ongoing dialogue. Set up privacy controls for conversations where the participants must be limited by necessity, while making sure that department- or company-wide dialogues are also able to take place on appropriate security topics.
Preserve institutional knowledge and be able to retrace steps that went into making security-related decisions. Be able to see the context around those decisions: How did we get here? Why did we make that choice then?

Store task lists for different scenarios where they can be easily assigned to specific employees and where accountability can be clearly traced back.

In a constantly changing system, with internal and external threats growing and appearing unexpectedly, there are two options: try to protect against those threats with static tools, or invest in solutions and cultural change that bring their own dynamic energy and built-in change and growth. Invest in communication and collaboration. Protect your data and assets by supporting the people in your organization so that they, in turn, can do their part as well.

Redbooth Private Cloud

To implement the recommendations described above, it can be helpful to have a software solution in place that offers you the ability to:

- Engage in secure chat across your company
- Link to documents that are automatically updated to the latest version
- Search conversations
- Put privacy controls in place where appropriate
- Assign tasks to specific individuals and track their progress
- Create, share, access, and modify task lists for repeatable tasks

With Redbooth Private Cloud, all of these features are included — and the entire solution is behind your own firewall, protected by the security measures you’ve put in place for your company. Many IT managers are able to install it on their virtual machines in under two hours.

To find out more about Redbooth Private Cloud and review the documentation, visit https://redbooth.com/private-cloud/.