The BoardVantage 4-1-1 Security Model

Whitepaper

Learn how BoardVantage's industry-leading security envelope comprehensively addresses platform security (external hacks, internal breaches, discoverability and human error), mobile security and service security.

At any given point in time my CTO or his team members are engaged in several dozen security conversations with prospective customers. Every one of those customers agrees that security is important, but rarely for the same reasons. Depending on who we speak with, we get very different views about what's important. IT tends to be focused on external hacks, GCs are more concerned with internal breaches and directors worry most about discoverability. The emphasis may shift from case to case, but this fragmented viewpoint is all too common. So out of necessity, we've become adept at explaining the finer points of view of these various parties to one another.

It is based on our viewpoint that the range of threats to confidential online communication is broad and that a good portal should protect against all of them. We also believe that the threat environment is rapidly evolving which necessitates a commensurately evolving architecture. This evolution needs to happen at the structural level.

We've implemented these principles in what we call our '4-1-1' model. That label serves as a mnemonic by categorizing threats according to their predominant character—platform, mobility and service model. Let's start with platform security.

Platform Security

The four major platform threats we harden against are 1) External hacks 2) Internal breaches 3) Discoverability and 4) Human error.

External threats include industrial espionage, social engineering and intrusion by non-state actors in various forms. We deploy proven techniques that include full strength encryption, multi-factor authentication, certificates, perimeter defense and secure site hosting to address them. This is a self-evident threat and IT departments are generally familiar with the countermeasures.

The second class of threats emanates from the inside. Internal breaches may come from disgruntled employees or others, often taking the form of sabotage or scandal mongering. Unacknowledged

system frailty here can become costly very quickly. Unfortunately, the potential for internal breaches does not have the same awareness in the IT community as external threats. Nevertheless we take it very seriously, because while it's true that much of the information that is communicated internally is not confidential, board content is in a class of its own. Its unique sensitivity dramatically raises the requirement for protection, whether protecting against threats from the outside or from the inside.

This brings us to discoverability. For many IT departments its severity is only now coming into focus. Perhaps that should not be surprising. Outside financial services, discoverability on internal IT systems is rarely seen as a serious concern. But when you ask a typical director, you get a different answer. For them discoverability is the number one concern when they think about electronic board communications. We deploy two key strategies to address this threat: 1) non-proliferation of content so that only a single copy of any document exists and 2) central administrative control which permits the GC to enforce the organization's retention policy independent from the actions of the users.

While the three threats I've discussed so far are intentional, the fourth threat is inadvertent—human error. As we all know, email and other common forms of digital communication are prone to oversharing but that approach backfires in board communication.

> ***So we designed the system to strike a balance between the need to share and the need to maintain control.***

Whether through segregation of content, granularity of permissions or hard restrictions on content distribution, the system is hardened so that common mistakes need no longer be a concern. We then apply modern interface technology with visual cues to make it easy for administrators to verify the results of their actions.

Of course the board portal business is anything but static. And with change comes new requirements for security. While platform security sufficed in a 'pre-iPad' world, the model has to be expanded to account for the risks introduced by the iPad's mobility. Fundamentally, tablet use requires the extension of the board portal's security umbrella to the device itself. This attribute represents the first '1' in our '4-1-1' model.

Mobile Security

Laptops may have been the accepted standard of mobile computing inside the enterprise for ten years, but this has not been the case in the boardroom. Although laptops have been present, they were not necessarily mobile. Directors would have one laptop at home, while the company provided a second one for meetings (even though most directors often stuck with paper). That pattern has changed with the advent of the iPad. Directors now carry their iPads with them wherever they go and they depend on them for many of their needs. That includes ready access to board materials even if they're out of Wi-Fi range. Also, in addition to reviewing documents they need an ability to annotate board material for personal reference. So the 'post-iPad' world has created heightened risk of discoverability. BoardVantage tackles this challenge with the Briefcase, which is built so any board content downloaded

by directors from the portal remains under the central control of the administrator. That means that the administrator can remotely delete any annotations. Even if a director neglects to delete his own notes, the GC can manage that task from the central administrative control, and delete the notes of all directors. This is not dissimilar to the practice of collecting and shredding all paper boardbooks after the close of a face-to-face meeting. Also, the Briefcase is encrypted and password-protected to safeguard its content in the event that the device is lost or stolen—content can then be centrally purged by the administrator.

> ***What we've effectively done with our Briefcase technology is bridge the gap between online and offline by extending our board portal security on the iPad.***

Without it, you run the risk of directors defaulting to consumer readers and annotation tools and subjecting the company to a range of serious risks, but particularly discoverability of their notes.

Service Security

The norm in the board portal business is third party hosting of board content. This is largely driven by the advantageous economics of the software-as-service model. Nevertheless, hosting can introduce a new risk. After all, you're trusting confidential information to a third party. Addressing this challenge is the second '1' in our '4-1-1' model.

Given what's at stake with board content, BoardVantage takes the position that it is not acceptable for any of our staff, whether in datacenter operations, engineering, or any other capacity to view customer data. That's why we built an architecture that encrypts all customer data on the server, which precludes this possibility. This is costly because it creates CPU overhead and it impedes the debugging process. However, it closes a serious hole in the security architecture of the hosted service model.

> ***At BoardVantage, we regard individual threats in terms of the broader threat environment and we study the cause-and-effect relationship between the various elements.***

The result is a framework that defends against all of them. The system built on that framework consistently meets or exceeds the security evaluations of enterprise IT departments including those of global financial institutions. As part of these evaluations we routinely submit our service to independent audits. These in-depth reviews, along with ongoing dialogue with a panel of IT departments in our F-100 customer base, assure that our standards and implementation remain at the highest level of commercially available security.

In this article I went into some depth on how our architecture protects against the various internal and external threats. In an upcoming article, I will discuss how we address the need for differentiated access among board committees and how we deal with the need for content segregation for senior executives, all with their own requirements for confidentiality.