Enabling a Collaborative Work Environment

Whilst keeping your critical information secure.
Introduction

Collaboration is essential for organizations to take advantage of high growth market opportunities, provide more tailored customer service and retain top-talent. There is no doubt that businesses today (knowingly or not to the IT team) rely heavily upon on collaboration tools, however, at the same time there is an ever increasing cost to pay for the agility and dynamic engagement. That cost has proven to be significant business risk. Here are a few points to ponder which will make you enable a more collaborative, but secure work environment.

As with most security projects there are three key components:

1) People
2) Policy / Process
3) Technology

Often there is a tendency to rush in with collaboration technology first and sometimes projects are created in order to 'try' new technology. Unfortunately, security is seldom thought about, let alone being one of the first things to be considered. The purpose of this brief document is to provide 'food for thought' around making collaboration more secure.

What's the point?

OK, so you have a project which requires collaboration, but let’s get down to basics. Answering a few fundamental questions will help you understand the security implications.

- Why are you doing this?
- What information is going to be shared?
- With whom?
- For how long?
- What are the risks and potential consequences for doing this?
- Does IT know?
- Should IT know?

The last point here is that often with cloud based collaboration tools no-one informs IT... and IT can help. They have probably been involved with collaboration tools in the past, and so may have a list of tools which are deemed to be ‘good’ from a corporate security perspective and if not, then they have the knowledge around what ‘good’ security looks like.

Collaboration Tools

The environment is all around collaboration, so you will need some tools to use, but which tools. For those with more advanced programs, there might be a list of already endorsed tools, if not then finding out what is in use is a great place to start – although getting people to change, when their choice is not secure, can be tough.

- What collaboration tools are you going to use?
  - Can this be done 'in the cloud', or do you need more control?
  - Several 'on-prem' (DMZ) applications that can work just as well

- Are they secure?
  - Is this more or less secure than if you did it 'in-house'?
  - Encryption? (Administrator override – or even more loss of control?)

- Are they available? (SLAs)
  - Work on the appropriate platforms? In the cloud?
  - Good uptime statistics?
  - Good backup / DR?

- Can you ‘see’ who has access, and when?

- Double check on information to be shared
  - Who is going to approve use?

- Create a list of IT sanctioned tools – and what types of project they can be used on

- Make a list of those tools which are not to be used.

So, which tools to suggest? Well, we all have our favourites including: Dropbox, Huddle, Linoma, Evernote and let’s not forget Office 365 and Google Apps. The reality is that you need something that suits your organization, and the people or partners who are going to use it.

Enforcement Tools

So you have chosen the collaboration tools, the next step is to look for enforcement tools that ensure that there is security around the collaboration tools. In general this is about ensuring that critical information which is not to be shared outside the company cannot be posted into an offsite collaboration tool.

- Infrastructure enablement... “Prepare to share”
- Policy flexibility & enforcement
- Keep the information safe
- No matter where it is
- Preparation around a secure collaboration framework assures agility and agility creates business advantage
Once there is a successful project which includes collaboration and enforcement tools this can form the basis of a collaboration framework. The framework can be used as a template for new projects as they arise, with the knowledge and understanding that this environment keeps critical information secure.

Which are the best enforcement tools? Again, it depends on the organisation, but for the leader in Adaptive Data Loss Prevention we would obviously recommend Clearswift, with solutions that go from email to the web to the endpoint.

For those who already have an email gateway solution, Clearswift’s ARgon for Email is a great way to integrate Adaptive DLP into an existing infrastructure without the need to rip and replace. Similarly for those with a web proxy, Clearswift’s SECURE ICAP Gateway will provide Adaptive DLP functionality without having to replace the proxy.

Updates
As with any computer application, keeping them up to date will reduce your risk from attack. Ensure that the collaboration and enforcement tools are kept up to date, as well as ensuring that browsers and plug-ins are also on the latest versions.

Audit
Just because this is a collaboration project, and potentially its hosted outside of your organization, doesn’t mean you can avoid the responsibility of the information safety. Decide who has this information and have them regularly audit the activity.

• Any new people given permission?
• Any large / anomalous data transfers?
• Who’s providing the value? Equal shares?
• Content becoming more sensitive? Time to move tools?
• Any security events raised, for example with inappropriate data being transferred to / from the site?

Project Lifecycle
All projects have a beginning, but quite a few don’t have an end, not because the project didn’t finish but because no-one shut down the project and the collaboration site. This leaves the information out there and therefore open to theft and misuse.

• Risk is proportional to access, the more people, the greater the risk... the longer the time the information is available, the greater the risk...
• When finished...
  – Delete the information...
  – Shut down the site...
  – Don’t reuse sites for different purposes as access control can become an issue

Policy & Process
Collaboration has become commonplace and the growth in tools makes it all the more important to have corporate policies and processes in place. Organizations should look to have the following:

• Collaboration process. (Inform IT, tool selection, audit, lifecycle, etc.)
• Collaboration breach process (when there is a problem)

People
People are both the strongest asset and the weakest link in the security chain. Getting employees, consultants and partners on side with a project improves the chance of success. For many security is an inconvenience until they understand the ‘Why’, so an education program is important, but it needs to go further than this.

• Why collaboration is good... but can increase risks...
• What collaboration tools are sanctioned
• The process to collaborate with external organizations...
• The process if something goes wrong...

Which department is responsible for people? It’s the HR department, or talent management or whatever name you have for that group. The HR department should become a key component to your cyber-security initiative as they interact with all the people in your organization from the CEO to the intern. While training is a key component, there is a lot more they can do:

• Training – new starters and regular refreshers for all employees
• Input to information security policies
• Acceptable use policies
• Policy communication
• Certification for key employees
• Data breach incident process
• Disciplinary process in the event of a breach

Summary
Secure collaboration is possible and with the right set of foresight around people, policies and supporting technology to create a framework which will enable business agility.

For all organisations, it is the protection of the critical information which is key. Critical information is the lifeblood of a business and provides differentiation and competitive advantage. Keeping it safe is of paramount importance.
Clearswift is trusted by organisations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and ‘adaptive’ data loss prevention solution, avoiding the risk of business interruption and enabling organisations to have 100% visibility of their critical information 100% of the time.

For more information, please visit www.clearswift.com.