

Finding a Balance between Security and Convenience

Communication with customers, vendors and business partners is the lifeblood of every bank. Without a doubt, e-mail and other Internet communication protocols are the most convenient methods of communicating and exchanging information with these parties. Unfortunately, they are all too often a source of critical data leaks as well.

Senior managers and IT Directors at banks are worried about compliance issues and meeting data privacy regulatory requirements. While establishing policies is fairly easy and straightforward, it can be quite difficult to actually enforce these policies and prove compliance to auditors. At Code Green Networks, we provide these senior managers with the peace of mind of knowing that their customers' personal financial information is not leaving the bank because our Content Inspection Appliance automatically enforces their anti-data-leakage policies.

In addition to critical customer data, banks must provide strong safeguards for other information such as: financial plans, salary information, employee files, contracts and legal documents, to name a few. One of our bank clients has taken a well thought out approach to solving this issue: they setup a secure information file folder in each department where all sensitive documents are stored. Our Content Inspection (CI) Appliance can then quickly and automatically 'fingerprint' these files so that they cannot leave the bank via e-mail, FTP, or Web mail accounts.

IT Departments appreciate this kind of convenient, hands-free monitoring, while CFOs really like the audit trail and affordability of our solution. It is especially useful in call centers that typically experience high turnover rates and are in direct contact with customers on a daily basis. Our content and data monitoring solution is ideally suited to prevent leakage in the call center, as well as with other member-facing employees.

For those e-mail communications that contain sensitive information that needs to leave the bank, we offer a link to a secure email server that will automatically encrypt outbound e-mails. It is also quite easy for recipients to receive and decrypt these secure e-mail messages because it only takes a couple of seconds to sign-in to view the message. With this kind of automatic monitoring and encryption in place, bank managers can be assured that their staff is always in compliance with the bank's security policies and responding in a systematic and secure manner.

In terms of implementation, our Content Inspection Appliance 1500 can be installed and configured to protect your sensitive information in an hour or less. Our engineers have designed our software with small to mid-sized banks in mind. The appliance is very easy to administer via a web-based graphical user interface. New policies can be defined and applied quickly and easily as the needs of the bank evolve. We believe that more and more banks will turn to Code Green Networks to help them monitor outbound traffic flows and automatically protect their customers' data and their own business information.



Chip Hay
Senior Vice President

Richard (Chip) Hay, Jr. is the Senior Vice President of Marketing & Customer Care at Code Green Networks. Chip joins Code Green Networks from Business Objects (NASDAQ: BOBJ) where he led the worldwide industry marketing team. Prior to Business Objects, Chip was a key member of the founding management team of Documentum that grew the company from a startup to market leadership and a successful IPO. Chip holds a Bachelor of Arts degree and PhD. from Northwestern University where he both taught and conducted research in information systems. Code Green Networks is a leader in developing the next generation of content protection solutions. Their products enable companies and government organizations to mitigate the growing threat of having sensitive information leaked from the inside using digital technology.