

**TRANSCRIPTION:**

**Xerox Thought Leadership Podcast Series**

Information Security and Compliance

Interview with Dave Drab

Xerox Global Services

**GM: Gabriele McLaughlin**  
**DD: Dave Drab**

GM: I am Gabriele McLaughlin from Emerging Technologies. On behalf of Xerox Global Services, I welcome you to Think Free with us. This podcast is part of an ongoing series. Be sure to visit [Xerox.com/ThoughtLeadership](http://Xerox.com/ThoughtLeadership) to download future podcasts.

GM: Today, I'm talking with Dave Drab. Dave is a thought leader at Xerox Global Services. He's an expert on security and compliance. Before your career with Xerox, Dave, I understand that you were an FBI special agent.

DD: Yeah.

GM: How valuable is information for companies today? Why does it need to be protected?

DD: Corporations today need to realize that there's a lot of information within the four walls of the enterprise that contributes to competitive advantage. Too often, this information is either ignored, or it's not fully appreciated, because it's not fully classified and understood—its value in the context of innovation and moving forward in the future. So, companies need to have the tools to be able to effectively capture and classify the information, and so they can effectively communicate it to employees, that this is the company's intellectual property. This is the company's future. When that's made clear, the opportunity for employees, or persons with access, to walk away with it is mitigated.

GM: From your current perspective in security and compliance, who is the enemy today?

DD: Hackers. Clearly, those individuals on the outside who are trying to break in, and unfortunately, in today's world, the playing field has been leveled so that anyone with a computer and access to the Internet can gain access to an enterprise's critical information assets. Organized crime groups are known to be collaborating with terrorist organizations. Foreign sponsored espionage operations are clearly targeting critical data of corporations. This is the body of external threats that has been able to leverage all of these global collaboration platforms that have provided enormous opportunity for businesses today. What we fail to recognize is the importance of understanding the threat from within, inside the enterprise. By those persons who have authorized access to their critical data and information within the enterprise. So, as we look at the challenge of securing a physical and digital environment, we recognize that this produces a strain of attack modes that are unprecedented.

GM: Can you enumerate some of the specific areas of vulnerability?

DD: Ubiquitous connectivity, the digitalization of critical information assets, the warp speed of technology being introduced into the enterprise environment, and the diversified global business models that companies are embracing today has introduced an unprecedented amount of risk to critical information assets. According to CIO and PricewaterhouseCooper's *2006 Global State of Information Security* in which they had surveyed over 7,700 executives

and security professionals worldwide, among their key findings was that most companies are reactive in nature rather than proactive and strategic. To merely react to what is occurring today is not good enough. You have to be strategic, you have to be focused, you have to understand what your threats are, who your enemy is, and you have to be in a position to identify vulnerabilities and implement appropriate controls to reduce or mitigate the risk of these threats.

GM: How about from a people perspective?

DD: In his book, *The World is Flat*, Thomas Friedman came up with three critical ideas that contributed to what he called a flattening of the world. This flattening occurred as a result of all of the technology changes, the telecommunication changes, the collapse of the former Soviet Union, all of these things contributed to the world we have today. With it was outsourcing, insourcing, offshoring, supply chaining, and informing. All of these collaboration platforms have been effectively leveraged by organized crime, terrorism, and foreign governments looking to steal critical corporate assets. What it means to the individual in his promise is that the globalization 1.0 was nations finding their place in the world. The dynamic was the nation. In 2.0 was the dynamic of the corporation in finding its way in the world, in its rightful place in the world. The 3.0 is the dynamic of the individual, which means that any individual in the world has the ability to compete on a global scale. Consider the security implication of this. Not only do you have to invent yourself to fit into this world, but you have to reinvent yourself. What does it mean to a company's critical assets if an employee realizes that he has to reinvent and move on to another company for

another opportunity? He's going to be inclined to siphon assets and critical information to build his resume in preparation for that next step.

GM: I've heard you say that security is too often a disabler. What do you mean by that, and how do we make it an enabler?

DD: It's a disabler because it's encumbering. It's something that is going to slow down the job. It's going to make it more difficult to get it done quickly, and security can be an inhibitor to productivity. The objective of a secure corporate culture is going to really turn that around, change the paradigm so that it's not a focus on productivity alone, because productivity without security is futility.

GM: Dave, what benefits will a company gain by adopting a holistic, people-centric approach to security?

DD: Security must be holistic. It must be comprehensive. It must go across the entire enterprise. It has to begin with a process by which you know and understand what your assets are. You identify threats to these assets. You investigate and determine vulnerabilities that you can close with regard to the management of your assets. It involves an ongoing process of education and understanding risk then selecting the right controls to mitigate the risk. This is a process that is unending. It is a process that requires expertise both inside and outside of the company. No one has all of the answers on security, and therefore it is important to have the right partnerships, the right kind of auditing, the right kind of testing to ensure that your security is sound. That what you have put in

place is effective in controlling unauthorized access or unintentional loss of critical assets.

GM: How about compliance?

DD: Well, good security is good business, and one of the derivatives of good security is compliance. Compliance is a component of security. Security, again, is the umbrella. It is vast in scope. It is considering all aspects of the enterprise, and observing and comprehending each of these elements is critical to having the right strategy, and once this right kind of approach is implemented, the benefits are enormous, compliance being one of them.

GM: Dave, is there anything else you'd like our listeners to know about security and compliance?

DD: We've talked earlier about intentional or malicious attacks on the enterprise, and realize that there are persons who are committed to breaking into an enterprise and stealing critical information assets. At the same time, much of the loss of critical information can be attributed to unintentional acts on the enterprise, whether it's human error or misconfiguration of critical devices. So, we realize that devices have to be properly configured so that there are not open ports that can be an attack vector. There have to be capabilities within the enterprise to ensure that the configurations comply with security policies that have been set in place for the protection of critical information on the network. Credible studies today indicate that attacks on the network are becoming more and more sophisticated, more strategic, directed at specific corporations,

systems, individuals, and devices. It's only logical that the weak link will be subject to attack. It's been my experience in interviewing persons who have confessed to breaking into enterprises as criminals or spies, that they would always tell us that, you know, you have all of these rules and policies in place, but you don't enforce them. So, what that says is that they are looking for the weak link, and that's how they'll exploit and gain access. So, we know that the hard-copy device environment, if improperly configured, can be that gateway, can provide a means of access to gain entry to the network to steal critical assets. Security is really about mitigating risk and reducing it to an acceptable level. So, when we look at the protection products, and techniques, and solutions that we have, we have to look at the amount of risk that a particular asset is facing. We have to consider the value of the asset, and then we have to look at the control of access to that particular asset, and then make a determination of what the acceptable and proper controls would be.

GM: Thank you Dave. If you'd like more information on Document Security and other important topics, join us at [Xerox.com/ThoughtLeadership](http://Xerox.com/ThoughtLeadership). I am Gabriele McLaughlin. On behalf of Xerox Global Services, thank you so much for listening.

[END OF RECORDING]