NELSON MULLINS

Privacy & Data Security Alert

January 3, 2019

Robert Rogers' Standing Orders of the 75th Ranger Regiment Adapted for Cyber Warfare

By David F. Katz

Robert Rogers was the forebear of the United States Army Rangers. His rules have been adapted and modernized and are featured in the United States Army Ranger Handbook. He led a light infantry force dubbed "Rogers' Rangers" and made his "28 Rules of Ranging," written in 1789, mandatory orders for his troops during the French and Indian War. The wisdom of this colonial frontiersman has applicability to cybersecurity and cyber warfare. Through careful analysis and thoughtful consideration one can easily draw modern lessons about how to best fight the cyber war that continues to threaten to engulf us all. Below are 10 of the "28 Rules of Ranging" that can best be adapted to a modern cyber war effort on the part of companies and the individuals in those companies responsible for cybersecurity.

1. **Don't forget nothing.**

Unfortunately, the lessons of the recent history of massive data breaches involving multiple sectors of the world economy are instructive for any prudent company. Studying where others fell short and how the affected companies responded in the face of tremendous challenges should be ingrained into every corporate executive and required reading material for every masters of business administration program in the country. Avoiding the mistakes of the past and remembering the disastrous results and pain associated with such breaches are powerful reminders of our collective vulnerability and the need to be vigilant and prepared for future attacks.

By analogy, preparation for engagement of the cyber enemy must be on everyone's mind within an organization. The underlying concept here is readiness and conducting operations on a war footing. If every individual was prepared to immediately respond to any cyber threat and constantly maintained the necessary tools to respond, the damage could be greatly minimized and at best prevented. The ability to respond quickly in the face of a daunting cyber event could mean life or death for the company. Preparation and readiness is the key to survival.

The message of this rule is powerful when considered in the context of cyber warfare. If you aren't proactively engaged in closely monitoring where your enemy resides and seeing them first, you are vulnerable. This means understanding the threat profile of your business operations and those that seek to attack the organization. In short, this means threat intelligence must be a regular part of your operations. As your business operates on a day-to-day basis (by analogy on the march) you need to be focused on seeing the enemy before they see you with excellent threat monitoring and threat detection capabilities.

Putting lying aside for the moment, the point of this rule is that accurate and timely communication is absolutely critical for those individuals on the wall and the front lines of the cyber war. Info Sec warriors are responsible for ensuring the company is secure and the risks are properly communicated up the chain of command to management. If there is a problem that creates an intolerable risk, it should be communicated truthfully and without hesitation in the interest of the larger organization. Having a dedicated and tested process for this reporting and encouraging a culture that enables such action can act to preserve the larger operation.

This is solid, logical, practical advice for anyone in any context, especially teenagers. How this exactly translates to the business operation speaks to how management and operational teams make decisions about balancing risk. The right calibration of "chance-taking" requires an understanding of all of the risks and the execution of good business judgment. Moving without caution into any innovation, new vendor relationship, or product line without a full appreciate of the cyber risk could be taking chances. This rule is universally wise and applicable but in the context of business risk may not easily transfer if the business objectives are driven without consideration to calibrated operational and cyber risk.

The concept communicated here is segmentation. Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks to maintain security, reduce an attack surface, and to limit movement across the network to other data repositories if compromised by an attacker. The wisdom here is to not be vulnerable to annihilation by failure to maintain separation. In general, understanding interdependent systems and how failure of one can lead to a crippling of operational resources, in the case of ransomware encryption for example, can lead to better planning and protection of resources.

An attack can cause chaos. A response plan is critical. Incident response plans are intended to help the organization operate effectively in the face of a "superior force" meaning a determined cybercriminal. Knowing how to regroup and how to focus a counterattack is an essential component to the response. Good planning, communication, and understanding how to recover can mean the difference between a successful response or a poor one. Everyone in the organization should understand their role in the response plan and the actions required of them when an attack occurs. This should be communicated on a regular basis across the organization.

Complacency is a killer. Failure to guard against attack is a killer. Unfortunately, companies do not have the luxury of standing down to cyber risk. As an organization grows or undergoes changes in its operations or shifts focus, it is easy to put the risks on the back burner until the main objectives are completed or prioritized ahead of others. Cybersecurity requires constant focus and vigilance no matter what else might be happening in the business. It is easy to focus on the things that make investors or customers happy or wealthy, but leaving yourself exposed can be costly. Engaging either internally or externally seasoned, experienced cyber "sentries," whether human or machine, is a sure way to avoid being caught unprepared and vulnerable during periods where your guard may be momentarily down.

You don't cross a river at a regular ford because that is where an attacker is expecting you to cross and where you're most vulnerable to an ambush. The analogy for companies is to avoid the tendency to take the easy way out when it comes to cyber preparedness. The market seemingly has a cure for every ailment, whether it is a new software tool or another product that promises security. There is no easy way out when it comes to security. There is no easy crossing of the river. Understanding the specific risks of the business and applying good practices even if they are operationally challenging or costly could make the difference. Following the herd can bring a false sense of security, complacency, and business "death."

1. **Don't sleep beyond dawn. Dawn's when the French and Indians attack.**

A company has to be honest with itself about whether its approach to cybersecurity readiness is analogous to a deep restful sleep. The point is that cyber criminals are lying in wait for you when you're most vulnerable and prepared to take the advantage. Understanding your company's "dawn" and ensuring you're up, moving around and ready to take on the coming attack can be directly correlated to management's focus and willingness to engage on cyber risk, active measures taken to mitigate risk, hiring and engagement with the appropriate experts, cyber liability coverage, and a detailed response plan.

View on Website

GET IN TOUCH

David F. Katz
Partner
T 404.322.6122
david.katz@nelsonmullins.com

