André Maginot's Line

Some time ago in this space, I used an obscure statement by a nearly forgotten British Prime Minister to make some points about cyber security.[1] As it happens, I studied the history of the period between the World Wars in my university days, so I often use some of the insights I gained in looking at then-current affairs when thinking about information security. I would like to turn now to a somewhat more famous artifact of the interwar years, the Maginot Line.

Here is what most people know: The Maginot Line was a series of fortifications near the French-German border intended to prevent German forces from invading France through Alsace and Lorraine, as Germany had done in two previous wars. Once those two nations entered into war again in 1939, the German forces went around the Maginot Line and invaded France once again. Thus, the term "Maginot Line" is today a catch-phrase for an expensive, foolhardy security failure.

The infamous line was named for André Maginot, a French politician who served in many cabinets in the 1920s and '30s, three times as the Minister for War.[2] Having spent much of his life in Lorraine, he was primarily concerned with protecting that part of France. He was not the visionary of the line; the idea came from the World War I French generals, particularly Marshal Henri Petain, the "hero of Verdun."[3] Neither was Maginot the leader who built the line; that was Paul Painlevé, his successor as War Minister.

So, what did André Maginot do? And what are the lessons of André Maginot and his line regarding information security generally (this is, after all, the *Information Security Matters* column), and cyber security specifically?

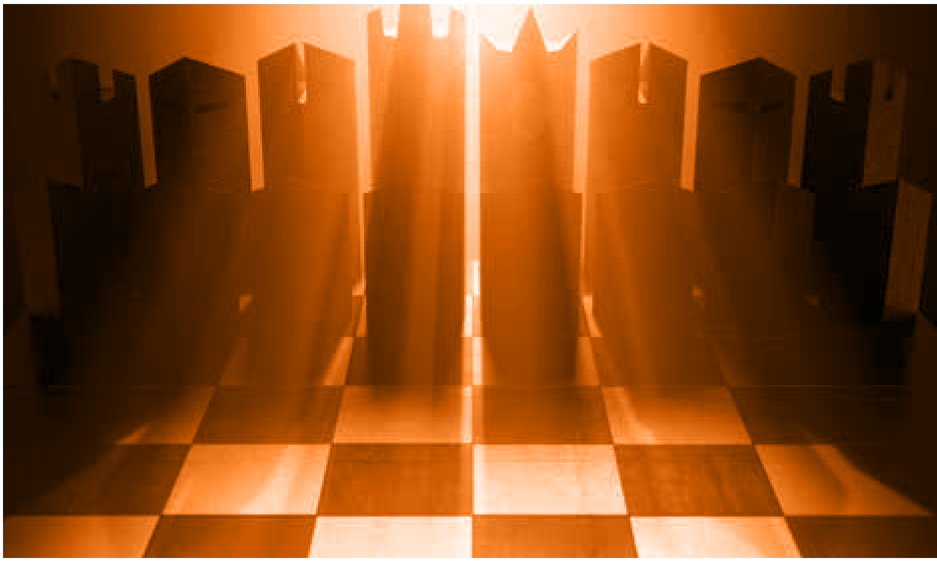
The Fallacy of Protecting Critical Resources

With the wisdom of hindsight, we know that the Maginot Line failed to protect France, but that was not André Maginot's primary objective at the time. He and the generals before him wanted to make invasion through Alsace and Lorraine impractical, if not impossible. And it worked! France was invaded in 1940 through Belgium instead. In cyber security terms, a strategy of protecting critical data resources, with less consideration given to so-called "Tier 2," simply exposes everything via the easiest route for an attacker to traverse. In other words, cyber security needs to treat the security of the IT environment holistically.

Moreover, it must be recognized that the methods of the cyberattackers are not monolithic and invariable. As an organization implements certain preventive measures, so those attackers intent on violating the integrity of information systems adjust their tactics. Effective antivirus filters once forced hackers to develop other forms of malware. Then, organizations became better at countering these new forms of hostile software. Now, it seems that the attackers are focusing instead on stolen credentials taken from authorized data users. This approach favors the antagonist in many ways: There is no need to find a zero-day or unpatched vulnerability, it is harder to detect, and it is more flexible once the credentials are used.[4]

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2shfuWv



Steven J. Ross, CISA, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

Enjoying this article?

- Read ***Transforming Cybersecurity.*** *www.isaca.org/cybersecurity-cobit*

Winning the Budget Battle Wins the Cyberwar

Maginot's great achievement was to recognize the spirit of his times, the *zeitgeist*, and take advantage of it. In an era marked equally by fear, pacifism and unemployment, he found it easy to appeal for funding of a line of battlements, a passive measure to strengthen defenses and create jobs at the same time. In fact, Maginot did not attempt to sell the line of fortifications as the sole or even the primary means of preventing invasion. He stated, "We could hardly dream of building a kind of Great Wall of France, which would in any case be far too costly. Instead we have foreseen a powerful but flexible means of organizing defense, based on the dual principle of taking full advantage of the terrain and establishing a continuous line of fire everywhere."[5]

> **"If we can gain the budget to make this war easier to fight and the risk easier to manage, that may be victory enough."**

Is any organization today prepared to build a Great Wall of IT? Even contemporary militaries do not have infinite budgets for cyberdefense (or attack, for that matter). What we are seeking is to take full advantage of organizing the preventive, detective and recoverability techniques we have in as economical a manner as possible and to establish a comprehensive program of cyber security. Budget monies are available with these wide-ranging, but nonetheless finite, goals. We may never "win" the war against cyberattacks, whatever winning means in this case. If we can gain the budget to make this war easier to fight and the risk easier to manage, that may be victory enough.

Cyber Security Must Align With the Culture

Even as the Maginot Line was being built, French generals realized that it might prove ineffective if it did not extend to the sea. But the Belgian government could not be convinced to build its own line nor would the French build one along its Belgian frontier. The political and economic environment would not permit more to be spent on preventing invasion.

There are political and economic environments within companies and government agencies that we often term the "corporate culture," within which there is a security culture.[6] Organizations will not, or cannot, do more for information security than that culture allows. Maginot understood that. Paraphrasing him in today's terms, the security culture within all organizations is the best safeguard against overspending (or underspending) on cyber security. "It controls not only the purse, but the man-power of the organization."[7]

Moreover, it appears that Maginot recognized that no one protective measure could win a war, although it could provide an essential edge in a battle, just as no one security tool is going to solve the problem of cyberattacks. Preventive software and hardware must fit within a technology environment that includes alarms and responsive triggers, analytics and recoverability. In addition, and closer to the context of culture, these tools must be incorporated into an organizational structure of monitoring and preparedness.

In one contemporary perspective, only slightly adapted, the Maginot Line was a dream, a hopeful dream full of security, warmth and promises. How many tons of cement? How many tons of steel? And how much money? Cyber security preventions, like the infamous line, may serve as a temporary measure to seal a potential breach. They can heal and even cure. But these protections can also die or become ragged.[8] It is for us security professionals to carry on this war, using the weapons available to us, constantly vigilant, with the strengths and limitations of our culture to guide us.

Endnotes

[1] Ross, S.; “Stanley Baldwin’s Bomber,” *ISACA® Journal*, vol. 5, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*

[2] Charles River Editors, *The Maginot Line: The History of the Fortifications that Failed to Protect France from Nazi Germany During World War II*, USA, 2015. The historical material on André Maginot and the Maginot Line comes from several sources. This publication is a good general discussion.

[3] And the traitor of Vichy.

[4] Schneier, B.; “Credential Stealing as an Attack Vector,” Schneier on Security blog, 4 May 2016, *https://www.schneier.com/blog/archives/2016/05/credential_stea.html*

[5] WebCite, “André Maginot: A History,” *www.webcitation.org/5kn33HV01*

[6] Ross, S.; *Creating a Culture of Security*, ISACA®, USA, 2011, p. 21. Will this shameless self-promotion never stop?

[7] Philip, P. J.; “Death of Maginot a Loss to France,” *The New York Times*, 8 January 1932. What Maginot actually said, as translated by the *The New York Times*, was, “Public opinion in all free democracies is the best safeguard against overarmaments. It controls not only the purse but the man-power of the nation. It is only in autocratic countries in which the people [sic] are not their own masters that armies and military caste become a menace. That is what happened in Germany in 1914. If we are still unconvinced that it will happen again we must be excused. Give us, and let us give Germany, time.” In finding this quotation, I was amazed at how much Maginot’s views from the early 1930s resound today.

[8] Greilsamer, L.; “De l’autre côté du mur,” (from the Other Side of the Wall as translated by myself), *Le Monde*, 28 January 2008, *www.lemonde.fr/idees/article/2008/01/28/de-l-autre-cote-du-mur-par-laurent-greilsamer_1004472_3232.html?xtmc=andre_maginot&xtcr=19*