“*A fake fortuneteller can be tolerated. But an authentic soothsayer should be shot on sight. Cassandra did not get half the kicking around she deserved.”*

– Robert A. Heinlein

We’ve been warning you about cyber threats and cyber security for quite some time. Surprisingly (to us) our articles have not proven to have been very popular, consistently scoring amongst the lowest in the site article analytics. We have been ringing the alarm bells about cyber security for nearly two years.

In November, 2009, we **wrote** that—

The AW&ST article reports that the U.S. is under such constant cyber-attack that ‘the definition of ‘success’ has shifted to containing intrusions instead of eliminating them.’ As SecDef Gates noted in a June 2009 memo, ‘our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security.’ … As the AW&ST article reminds us, our adversaries are making advances as well, perhaps in areas in which we are vulnerable to exploitation.

A month later, we **reported** on the U.S. Cyber Challenge, a nation-wide contest that was designed to “ find 10,000 young Americans with the interests and skills to fill the ranks of cyber security practitioners, researchers, and warriors. Some will become the top guns in cyber security.” The United States needs such “cyber warriors,” of course, because it’s tough to defend (or attack) when one lacks resources. We have consistently pointed out that the Pentagon’s over-reliance on tanks and aircraft and missiles is missing the point that the information grid and its infrastructure are its unprotected flank.

In January 2010 we **asserted** that—

The next big war between nation states probably won’t be fought using tanks and planes; it will probably be fought in cyberspace. The war could be over before a single shot is fired, with the winner being the first to shut down the other side’s electrical and information grids. The soldiers of the next war are in training now. And the United States is way behind other nations in training and equipping its cybersoldiers.

Finally, we **noted** the following—

We certainly don’t want to be seen as being overly alarmist. So, we’re just saying that the so-called “Iranian Cyber-Army” “may have successfully infected as many as 20 million PCs.” Our cyber-security stories don’t interest many site visitors for some strange reason, but here’s a link to the story at computerworld.com. Again, there’s no reason to be overly concerned about this group, which may or may not be connected to the Iranian government, but which is known for having hacked both Twitter and Baidu. Don’t be worried about its for-rent botnet service. Ignore the fact that investigators found ‘an administration interface where people who want to rent the botnet can describe the machines they would like to infect and upload their own malware for distribution by the botnet.’ …

And while you’re not looking at your lack of cyber-security, take no notice of Darnell Albert-El, of Richmond, Virginia, who was sentenced to serve 27 months in prison for ‘hacking into his former employer’s website’ and ‘one count of intentionally damaging a protected computer without authorization.’ Albert-El, a former IT Director for Transmarx, LLC, was fired by his employer. After his termination, ‘he used a personal computer and an administrator account and password to access the computer hosting the Transmarx website.’ What did he do with his unauthorized access? He ‘caused the transmission of a series of commands that intentionally caused damage without authorization to the computer by deleting approximately 1,000 files related to the Transmarx website.’ ….

So when we **heard** (in March 2011) that EMC’s security division, RSA, had been hacked, we were hardly surprised. RSA, for those scratching their heads in puzzlement, is the self-proclaimed “premier provider of security, risk, and compliance solutions for business acceleration.” According to its **website** , RSA “brings visibility and trust to millions of user identities” by helping businesses implement “controls in identity assurance, encryption and key management, SIEM, data loss prevention, and fraud protection.” Except the company founded on computer security found itself the victim of an “extremely sophisticated” exploitation scheme that stole “information related to the company’s SecurID two-factor authentication products.”

As they say, “Physician, heal thyself.”

According to this **Wired article** , “SecurID adds an extra layer of protection to a login process by requiring users to enter a secret code number displayed on a keyfob, or in software, in addition to their password. The number is cryptographically generated and changes every 30 seconds.” The Wired article also reported—

‘While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers,’ RSA wrote on its blog, ‘this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.’

As of 2009, RSA counted 40 million customers carrying SecurID hardware tokens, and another 250 million using software. Its customers include government agencies.

Well, RSA’s assessment of the situation proved to be—shall we say?—overly optimistic.

On May 21, 2011, less than 60 days after the EMC penetration, aerospace/defense giant Lockheed Martin was attacked in a “tenacious” manner. According to this **Financial Times** article—

Lockheed did not confirm that the raid on its data built on the attack on RSA, but many analysts said that it was likely, because one of Lockheed’s first acts had been to disable the remote logins.

More disturbing, they said, was the fact like others in the defence industry, Lockheed had previously acted to make itself less dependent on the rapidly-changing numeric passwords the RSA tokens produced.

The RSA breach began with e-mails sent to its staff with an attachment that contained a hidden remote-access program that took advantage of a security flaw in Adobe’s Flash software for viewing content. …

Analysts said it appeared the hackers had obtained the ‘seed’ numbers used to generate passwords. If they combined that with administration information kept by customers associating tokens with specific employees, the passwords could be duplicated.

The National Security Agency went further, declaring not long after the RSA attack that the tokens should no longer be deemed sufficient to grant access to ‘critical infrastructure’. Defence contractors including Lockheed began requiring employees to put in extra personal passwords.

Although Lockheed said its programs and customer data had not been compromised in the attack, the breach suggests that the extra passwords were not sufficient to repel hackers, an ominous sign for remote-access systems in defence and other industries.

Richard Stiennon, a former Gartner security analyst and author of a recent book on cyberwar, said: ‘If there is a direct connection between the RSA breach and the subsequent attacks on Lockheed Martin and other defence contractors, this will be one of the most sophisticated sequences of attack events ever’.

But that’s not all—not by a long shot.

Reports have recently emerged that both Northrop Grumman and L-3 Communications may also have been victims of similar cyber-attacks. One news story reported—

Attackers hit major defense contractor L-3 Communications Holdings by spoofing pass codes from a cloned RSA SecurID token, Reuters reported May 27. The attackers may have used a similar method to target another defense contractor, Lockheed Martin, on May 21. The second-largest U.S. defense contractor Northrop Grumman may also have been hacked, as the company shut down remote access to its network without warning on May 26, according to Fox News. …

‘L-3 Communications has been actively targeted with penetration attacks leveraging the compromised information,’ an L-3 executive wrote April 6 in an internal memo obtained by Wired Threat Level .

It’s not clear from the internal email whether attackers managed to actually break into L-3 networks, or if they were detected in the midst of the attack. The memo also did not specify exactly why or how L-3 came to the conclusion that the SecurID two-factor authentication system was at fault. An L-3 spokesperson just said the company takes security seriously and that the incident has been resolved.

While the details of these attacks are not “fully known,” it is likely that attackers were able to install a keylogger somewhere within the network, according to Harry Sverdlove , CTO of security firm Bit9. The information captured and knowledge of RSA’s token-generation algorithm would give attackers a way to breach the network, Sverdlove said, noting that this would be a “worst case scenario” for SecurID.

‘It would mean that a single point of attack can be used to defeat the dual-factor authentication provided by the security tokens,’ Sverdlove said. The keylogger may have been installed on a remote system that connected to the network via a VPN. This makes sense, since the ‘best bet’ is to attack vulnerable endpoints, or computers that are connecting remotely and are likely not under the direct control of the organization’s security policies.

Northrop Grumman does not comment on cyber-attacks against it, the company spokesperson said. It’s also unclear how Northrop Grumman was hit, as ComputerWorld reported that the defense contractor replaced all its SecurID tokens with tokens from a different vendor ‘immediately’ after the RSA breach.

The network shutdown at Northrop Grumman caught ‘even senior managers by surprise’ and caused chaos, according to the Fox News story. ‘We went through a domain name and password reset across the entire organization,’ an unnamed source told FoxNews.com.

Okay. If that were all we had, you might be a little concerned. But we’re not done yet …

This past week, the International Monetary Fund (IMF) was **attacked** . “The hack's perpetrators obtained a ‘large quantity of data,’ including e-mail and other documents during the intrusion, according to
Bloomberg

.” The report continued—

How hackers were able to penetrate the IMF's network is still unknown. But it appears the intrusion may have been the result of a spear phishing attack. This kind of attack typically works by tricking an employee into clicking on a link to a malicious website or downloading a file loaded with malware.

And, on June 11, 2011, the hacker collective **Anonymous** called-out the North Atlantic Treaty Organization (NATO), according to **Time Magazine**. According to Time, Anonymous issued a response to a recent NATO report on the perils of cyber warfare by telling NATO, “This is no longer your world. It is our world—the people’s world.”

Anonymous’ manifesto continued—

We do not wish to threaten anybody's way of life. We do not wish to dictate anything to anybody. We do not wish to terrorize any nation.

We merely wish to remove power from vested interests and return it to the people - who, in a democracy, it should never have been taken from in the first place.

The government makes the law. This does not give them the right to break it. If the government was doing nothing underhand or illegal, there would be nothing 'embarassing' [sic] *about Wikileaks revelations, nor would there have been any scandal emanating from HBGary. The resulting scandals were not a result of Anonymous' or Wikileaks' revelations, they were the result of the CONTENT of those revelations. And responsibility for that content can be laid solely at the doorstep of policymakers who, like any corrupt entity, naively believed that they were above the law and that they would not be caught.*

A lot of government and corporate comment has been dedicated to 'how we can avoid a similar leak in the future'. Such advice ranges from better security, to lower levels of clearance, from harsher penalties for whistleblowers, to censorship of the press.

Our message is simple: Do not lie to the people and you won't have to worry about your lies being exposed. Do not make corrupt deals and you won't have to worry about your corruption being laid bare. Do not break the rules and you won't have to worry about getting in trouble for it. … Do not make the mistake of challenging Anonymous. Do not make the mistake of believing you can behead a headless snake. If you slice off one head of Hydra, ten more heads will grow in its place. If you cut down one Anon, ten more will join us purely out of anger at your trampling of dissent.

Now you should be nervous.

Our take (besides our repetition of the need to enhance cyber security)? We think we are all watching history being made. We believe that 2011 will one day be noted for the beginning of the cyber-wars.

No, we don’t think we’re being overly alarmist. Just ask Lockheed Martin, or L-3 Communications, or Citigroup, or the IMF. Our website was attacked and wiped-out a few weeks ago—and we had taken the precaution of blocking all IP addresses based in China. (Fortunately, our back-ups worked and we were up and running again within 72 hours.)

We think the U.S. has fallen behind other countries, and parastatial entities, in the strategy and tactics of cyber-warfare. Like the French and their Maginot Line, the U.S. has spent billions on its military assets, without adequately securing the information grid that is the true backbone of its high-tech military. We think the U.S. military is vulnerable; we think corporate America is vulnerable. And we’re pretty sure you are vulnerable as well.