With a constant barrage of news about high-profile cyber attacks, 2013 was one of the most interesting years ever in the security arena. Headlines seemed ripped from a Tom Clancy novel: targeted cyber espionage by one country on another; state-sponsored attacks on businesses to steal intellectual property; cyber attacks designed to disrupt and embarrass governments. Hacktivism, cyber espionage, and cybercrime have become the norm. And the intensity of attacks has escalated.

With targeted attacks, analyzing the targets is as important as revealing the perpetrator. This backgrounder examines the most-targeted vertical segment in Europe—namely, government—and the implications for today's threat landscape.

Typically, government is one of the most targeted verticals in Europe. This continues to be a major problem around the globe. Nations target other nations to steal state secrets. Tech-savvy activists subvert government websites to protest national policies. And cybercriminals aim to pry open the treasure trove of citizens' personal data on government systems.

Making matters worse, many governments operate as a large, interlaced web of independently run agencies. Many of these agencies lack the know-how to lock down and harden their systems from even simple attacks. It's no wonder that advanced persistent threats (APTs) are so successful when aimed at this large and unwieldy segment.

Here are the most-targeted verticals in Europe for 2013 according to FireEye research:

1. Government
2. Healthcare/Pharmaceuticals
3. Financial Services
4. Energy/Utilities/Petroleum refining
5. Services/Consulting/VAR
6. Telecom (Internet, phone, and cable)
7. Chemicals/Manufacturing/Mining
8. High-tech
9. Consumer products and Retail
10. Higher education

For cybercriminals, the Internet is a low-risk, high-reward way to swindle information, whether for profit, power, or political advantage. In December, FireEye reported on Operation Ke3cheng, a Chinese effort to steal diplomatic information from European Ministries of Foreign Affairs. The lesson is clear: Many European governments are still not able to block advanced cyber attacks. Even among modern Western governments, cyber attack preparedness varies. To bolster their readiness, many countries are assessing a number of areas, including cyber program maturity, policy maturity, process maturity, and security awareness.

How is Europe doing? So far, results are mixed. Cyber security is an intricate challenge, thanks to the region's vast geography, mishmash of different policies and cultures, and a still-fledgling economic recovery in many parts of the region. The good news: Many European governments are beginning to recognize that today's advanced attacks are not going away.

Coming to this realization, many European countries have begun to adopt recommendations such as the United States' National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4. The document prescribes security controls for [U.S.] federal agencies' IT systems (and those of anyone working with [U.S.] federal agencies).

The newly added Security Control 44 recommends "detonation chambers" to execute file attachments entering a network to ensure they are not malicious.

This type of forward thinking is growing more common in the UK, France, Germany, and a number of other countries. While the widely cited defense-in-depth model has merit, more and more officials realize that it is not impenetrable. A truly robust defense requires new security methodologies to keep nation-state attackers at bay.

EU-member countries have begun to share these new concepts with one other through NATO and related think tanks such as the Cooperative Cyber Defence Centre of Excellence (CCDOE) in Estonia. The recent launch of cyber exercises by NATO will help EU officials better understand cyber attacks and how to build a security infrastructure to detect and stop them.

Modernizing the way government and industry work together on security issues and share threat intelligence is another critical step. The recent launch of the European Cybercrime Centre and the adoption of the EU Cyber-security Strategy will also help strengthen Europe's defenses. Programs such as the Cyber Security Information Sharing Partnership (CISP) in the UK are also a great start to managing today's advanced threat landscape. Many of these initiatives in Europe have given it an advantage over other industrialized regions around the world.

We hope other governments mirror these efforts. The key to reducing the impact of future attacks may well be information-sharing partnerships between government and industry. By building a deep level of trust, government and business can help foster a safer environment without cumbersome and costly regulation.

Governments must view cyber attackers as they would any other threat—one that changes and evolves in a never-ending arms race. They need policies, procedures, and structure to counter these threats. Officials must build systems with proactive security in mind. Moreover, they must continually review their security plans to ensure they can counter ever-changing threats.

Preserving the conventional enterprise mindset—where new technology is reviewed and updated on a three- or five-year cycle—all but guarantees that attackers win. And failing to update traditional defenses is tantamount to surrender.

Today's advanced threats exploit zero-day vulnerabilities that easily sidestep yesterday's signature-based defenses. Legacy solutions and even newer file-based sandbox analysis cannot detect advanced attacks, let alone stop them.

Governments face a growing deluge of cyber attacks that are growing increasingly sophisticated, stealthy, and dangerous. These threats are here to stay. That is why governments must rethink their security posture to meet today's cyber challenges.