iboss™
CYBERSECURITY

Guidelines for **Increasing Public Sector Cybersecurity**

The **Challenge**

The cybersecurity threat landscape today is more fluid, more dangerous, and more organized than ever. Hundreds of thousands of new threat signatures are produced daily, ransomware is rampant and, perhaps most disturbingly, organized crime has turned malware into a business complete with human resources departments, customer service, and money-back guarantees. They even offer technical support! Worst of all is they operate from enclaves inside countries with either relaxed, non-existent, or unenforced laws regulating their activities. This makes stopping this cyber tsunami at its source almost impossible.

Today's cadre of hackers are after one thing: money – and lots of it. It would make sense that going after banks would be the fastest and most lucrative way to get it, but this is not the case. Data, specifically the personal information held in myriad State, county, and municipal databases, is just as valuable – if not more so – than pilfering bank accounts directly. So like Slick Willie Sutton, the 1930s bank robber who, when asked why he robs banks replied " … because that's where the money is", cybercriminals are going after government databases with because that's where the data is.

There are a couple of very good reasons for this: governments hold data on everyone and every business. And that information is stored in databases – some secure, some not – spread across hundreds of departments, datacenters, and geographies that are accessed and accessible by tens of thousands of employees, devices, and applications. This gives hackers almost unlimited vectors from which to launch an attack. Adding to the problem is these databases are often protected by outmoded and outdated methods such as firewalls, which alone, can't provide sufficient protection against the sophisticated attacks mounted by today's cyber criminals.

Unfortunately, many in state government either have their hands tied by bureaucratic hurdles or their heads in the sand when it comes to dealing with these new threats. According to the National Association of State CIOs (NASCIO), chief information security officers are also challenged by a lack of funding, the ever-increasing sophistication of emerging threats, and a shortage of qualified cybersecurity professionals.

To make matters worse most government chief information officers (CIOs) and CISOs are dealing with a patchwork of old and new technologies that were never designed to work together. As government's move to embrace shared services, mobile computing, and cloud based services, this has led to a mosaic of custom coded and vendor supplied workarounds that introduce yet more security headaches.

> **The message presented is alarming and it is clear,"** say the authors of the *Advanced Cyber Analytics: Risk Intelligence for State Government* report. **"Government and industry must develop a proactive, forward looking strategy for dealing with cyber threats… States have no choice but to acquire, prepare and exercise new advanced capabilities to fight cyber threats."**

Additionally, organizations and governments are allowing all manner of smartphone, laptop, workstation, and operating system access to their networks. Country health workers, social workers, and state inspectors, for example, use smartphones, tablets, and laptops in the field that are vulnerable to data loss via cyber attack and physical theft. In some instances, these may be personal devices already infected with malware. Add to the mix the push for more and more web-based, citizen self-service and you have a network full of holes.

These holes in turn lead directly to a network core that may or may not be hardened against new types of attacks – specifically, ransomware and advanced persistent threats (APTs) that can reside on the network for months before being activated via a remote command and control server in some far off corner of the globe. Or, like a cancer, shape-shifting polymorphic malware simply hides in plain sight, spoofing the existing security apparatus into thinking they are not there.

Another major difference between government and corporate networks is the sheer amount of personal and financial data that governments hold on everyone, including businesses. This is because supplying this information is compulsory. With the exception of perhaps Google, even a large, global corporation's information assets cannot begin to compare to this vast personal data store.

And where a large corporation will seek to centralize, control, and encrypt much of their most sensitive data, government, because it's mission is not profit but service, tends to lean in the opposite direction; favoring openness and access. This means data tends to be widely accessible and shared among many different departments, quasi government organizations (like a county run hospital), contractors, private citizens, and government employees just doing their jobs. This makes controlling and protecting government data that much harder while simultaneously providing a target-rich environment for hackers.

Government CISOs are also challenged by a budget process that is not geared towards countering the fast-moving nature of today's ever-evolving threat landscape. Budgets are often set on an annual or biannual basis and requests for additional funding to meet immediate needs (even emergency ones) are often delayed by the various committees and decision-makers that hold sway over the process.

Compounding the problem is most managers and administrators (even those inside IT) have very poor visibility into where IT's budget really goes. Because of this, they feel compelled to rein in IT spending wherever possible.

And because risks are sometimes evaluated based on the cost to clean up a data breach versus preventing one, finance managers won't spend money up front to preempt an incident. Of course, this does not take into account the potential costs to the individuals whose data has been pilfered. Nor does it factor in the potential litigation costs of a data breach, which are increasing.

Added to this is the fact that keeping up with the latest zero-day exploit or rootkit is a daunting task, considering how much government IT administrators have on their plates. Added to that is that fact that they may not have sufficient appreciation for the damage a major cyber attack can cause.

An ominous warning to this effect can be found in a recent NASCIO report, *Advanced Cyber Analytics: Risk Intelligence for State Government*, which states: "It can be presumed at this point that state government systems are infected with a myriad of rootkits that haven't surfaced yet. They [the rootkits] are still being traded like the financial markets trade futures. The longer malicious software remains undetected in a computer system; its bid value goes up – it becomes more valuable to the enemies of government organizations."

In the business world, cyber-security spending is driven by the fear of such an occurrence and the fear that failure to act preemptively will lead to irreparable brand damage, a loss of customer trust, painful regulatory action, lawsuits and fines and, ultimately, a loss of profitability and shareholder value. Governments have no such concerns. A massive data breach will not keep people from sharing data with them. And, while litigation is expensive, it will not materially affect day-to-day operations.

This does not mean that the people in government don't care. They do. They understand there is an unwritten contract in this country that says the government will do what it must to protect its citizens. This trust is essential to the smooth operation of government. But it's more than that. Like the rest of us, they want to do good work, be recognized for it, and advance their careers. A massive data breach is not a good resume builder, after all.

So the incentives are there. Now the question is what to do about it.

The **Solution**

It is no longer effective to rely entirely on perimeter defenses such as firewalls, anti-virus, mobile data management, and network-based intrusion prevention (IPS) and detection solutions (IDS) that only block known exploits or tell you that you've been compromised after the fact. Threats today move too quickly and come from too many different directions for this "castle-doctrine" approach to work.

Nor is it possible to lock down all of your data using encryption. While this would be a highly effective way of preventing most hackers from accessing sensitive information, it would be useless against ransomware, the fastest growing category of malware. This is because ransomware simply encrypts already encrypted data, too. Because this data is so widely shared for use in a multitude of systems accessed by myriad endpoint devices using all manner of operating system, it would severely limit the usability of that data.

Today's cyber criminals have graduated from the easily detected smash-and-grab tactics of earlier times. The malware they create can sit on a network unnoticed for months or years quietly watching and waiting for the right time to launch its payload. This dwell time is a hallmark of the APTs that high-value targets such as governments must contend with.

So if building walls higher and digging moats deeper isn't the answer, what is?

Most security experts today will tell you that the best defense is a good offense – that you have to anticipate your opponent's next moves if you are to get out ahead of them. The first step to meeting these threats head-on is identifying the most sensitive data and taking immediate steps to secure it. This means deploying all the available security measures: behavioral-based outbound data loss prevention (DLP) analysis, strong authentication protocols and access policies, virtual private networks (VPNs) to protect data in transit, ongoing employee education, hiring seasoned security professionals, conducting regular backups and DR drills, reviewing patching procedures, and so on.

In the cyber world security must integrated and multi-faceted, with each solution working to reinforce the next. So, while firewalls are still necessary, for example, an integrated approach would secure all network ports instead of just 443 and 80, which are the default ports used for two-way communication with the public internet.

In an integrated approach, network traffic analyzers would do more than just generate thousands of alerts that may or may not be followed up on by overworked security admins who can't possibly look into all of them. An integrated approach functions automatically in the background to isolate attacks, sandboxing suspicious activity such as command and control (C&C) callbacks from TOR browsers and the dark web – before data leaves the network. An integrated solution uses pattern recognition and analytics to distinguish between normal and the abnormal network traffic that signals an attack is underway. An integrated approach allows for the selected decryption of SSL traffic coming in from the web, an increasingly important ability given that most cloud applications communicate with users via SSL tunnels.

In fact, many security best practices have nothing to do with technology. They start with policies and procedures that are enforced and backed-up by technology. While an integrated solution takes into account all of these things, it focuses first and foremost on data. This allows security teams to be more pro-active, using real-time reporting and dashboards to spot attacks in their very earliest stages, when data exfiltration is just beginning. This not only gives them the ability to isolate attacks quickly it provides them with the time they need to reverse-engineer an attack so they can trace the hack to reveal its full extent and, hopefully, for purposes of prosecution, back to its source.

Conclusion

As anyone inside the cyber-security world will tell you the question today isn't if you've been hacked, it's when will you find out about it. While countering cyber attacks is more challenging than ever before, security pros in every industry, including government, can gain the upper hand by going on the offensive.

By adopting a proactive approach to cyber security that takes into account all available options – technical and procedural as well as training and policies – to create a multi-faceted, integrated, and self-reinforcing system that stops attacks before they begin.

About
iboss Cybersecurity

iboss Cybersecurity defends today's large, distributed organizations against targeted cyber threats which lead to data loss, with the next-gen iboss Cloud Secure Web Gateway Platform, leveraging patented advanced threat defense technologies delivered 100% direct-to-cloud. iboss' unique cloud architecture provides each organization with its own container, so that a customer's data is never mixed with any other's in the public cloud. Our advanced security solutions deliver unparalleled visibility across all inbound/outbound data channels, and include security weapons that reveal blind spots, detect breaches and minimize the consequences of data exfiltration. With leading threat protection and unsurpassed usability, iboss is trusted by thousands of organizations and millions of users worldwide.

iboss, Inc. · 877.742.6832 · sales@iboss.com · U.S. HQ 4110 Campus Point Court · San Diego, CA 92121