Are you ready for the next attack?  
(Part 1)  
Reviewing the SP Security Checklist  
Barry Greene - bgreene@senki.org  

As many of my colleagues know, I’m constantly on the look out for tools that would help my peers in all networks find ways to mitigate the security risk in their operations. At MYNOG 5 (www.mynog.org) I reviewed the latest tool, a checklist operators can use to prepare their network for before the next security attack. This post is part 1 of a two-part post accompany the MYNOG 5 presentation. Part 1 will review the threat and context for why Service Providers and big networks need to act. Part 2 will get into the checklist in a way that can be used by operators.

Why Checklist?

Checklists are one of the most essential tools for productivity we have in the industry. Some will call these “standard operating procedures,” but for anyone who lives with Checklist, you will know that they go beyond SOPs. Checklists are tools that drive the operations. Checklists are used every day. Checklists are continually improved - using the lessons learned to continuously improve the tool. Talk to any pilot on how checklists are critical for their work. For those who are new to Checklist, please pull down and read The Checklist Manifesto by Atul Gawande. If you don’t have time, search on YouTube for a talk or check out the TED Talk here: http://www.ted.com/talks/atul_gawande_how_do_we_heal_medicine.

Surprisingly, too few “Internet” and “Telecom” operators use the checklist approach to optimize their operations. This can be easily corrected. What follows is the continuation of checklists that can be used by operators - be they Mobile, traditional Telco, Content, of ISPs. They will be designed to be cut/pasted and used in your organization’s checklist. The objective is to help operators take action by saving money. Many of the items in these checklists are things that would be “recommended” by high end “security consultants.”
(Additions to the checklists are always welcomed. Just E-mail to bgreene@senki.org).

Why Should I Care?

"[T]he malware that was used would have gotten past 90 percent of the Net defenses that are out there today in private industry and [would have been] likely to challenge even state government," - Joe Demarest, Assistant Director - US FBI’s Investigation’s Cyberdivision.

The state of security throughout the industry is horrendous. It is essential that we deploy new technologies to interconnect, but it is also apparent that the tools we have to secure our networks are not working. Why is this happening? Part of it is the reality of interconnections and the limitations of civil society to push back on “cyber-crime.” In most of the world, civil society determines the level of crime that is tolerated in their community. Laws, police, governments, citizen activism, courts, jails, and public policy all are factors that push back against crime. We have clear borders in the world that define the sphere of control and the ability to push back on crime.

This is not the reality of the Internet. Civil society has little to no ability to push back against crime on the Internet. Two factors are essential to understanding why this is a problem. First, in the world of Telecommunications and the Internet, we do not have “countries.” We have Autonomous System Numbers (ASNs) which describe networks. The organizations for which these ASNs are assigned can only control what is happening on their networks. Many of these ASNs cross borders across the world. Some are global, crossing every country. This creates a problem where a country has challenges imposing “Internet borders.”

The second factor is related to the global reach of the Internet. A criminal sitting in one country and reach out and connect to someone in many other countries. They can proxy through and “bounce” off 3rd party countries - hiding their source to the
organizations they are victimizing. How would a civil society push back against crime when there is little to no chance to “attribute” a crime to a particular criminal. Even when the crime can be traced to a criminal in another country, how would international law allow for extradition? In essence, the traditional factors civil society uses to push back against crime will not work on the Internet (or in the telecommunications world).

The reality is “cyber-crime on the Internet” will be a persistent risk until we have international law and judicial system that allows for the global civil society to push back against “International cyber-crime.” This may happen, decades in our future. Until then, anyone connected to the Internet must be mindful of the risk and assume that there is always someone trying to own elements on your network.

The Threat is a Force of Nature

If the cyber-security threat is something that cannot be solved in the foreseeable future, organizations will need to rethink how they approach “security” throughout their operations. Luckily, one approach is an approach that is known to work in the industry - ensuring cybersecurity in the same way one would insure against natural disaster. If we look at cyber-security as a force of nature, options and approaches to mitigate risk can be used to mitigate the cyber-criminal threat. Like a hurricane, tornado, earthquake, or flood, cyber-security is not a matter of if, but when. The risk is something that is a well-known business risk that will impact the company at some time. The first thing that companies do to mitigate the “force of nature” risk is to buy insurance against that risk. The company would sit down with several insurance companies and compare options that would cover the risk if a force of nature event impacting their operations.
We do have an emerging cyber-security insurance offering in many parts of the world. These insurance companies would have an assessor who would review the organization for the potential “cyber-risk” and apply a premium appropriate to that risk. The initial premium would be steep. How do you reduce the premium? Use the insurance company's checklist of actions that they deem would mitigate the risk. Checklists and "compliance list" are a well-used tools that are designed to reduce the risk and reduce the premium cost to mitigate that risk. In some ways, insuring against natural disasters have a well-defined approach on the return on investment for each item on the "checklists." If it reduces the premium, then it is worth the investment. (Note the impact of cyber-insurance would be a future post).

Focus on the Real Threat

There is a lot of confusion on the real security threat to an organization. Some would say that there is no need to focus on the threat (i.e. the human being launching the attack). This thinking is dangerous. It will lead organizations to concentrate on the wrong problem.

Think of the problem this way. Someone comes into a bank with an AK-47, holds up the bank, steals $500,000 dollars, and gets away before the police can catch them. The police now post a bulletin to everyone describing the AK-47, what color was the stock, how big was the ammunition clip and all the interesting extra features on the AK-47. There is nothing about the human who held the AK-47 and did the criminal act. How would that seem to the public? Police would get fired.

But, this is what is happening today in the “cyber-security” community. There is a lot of information about the malware, botnets, and other tools used to perpetrate the crime, but petite information that tracks the crime to the "human" source.
Companies who get DDOS defense are satisfied with “Anti-DDOS” solutions that allow the companies to ride out the attack, but do very little to trace back the attack to the humans who have launched the attack. DDOS is either extortion, retribution, or vandalism. There is no difference between a human which threatens to break your leg with a baseball bat unless you pay for protection and a DDOS extortion who says pay to keep the site from going down. Both are acts of a human. Don’t focus on the baseball bat, concentrate on the criminal holding the baseball bat. Focus on the criminal holding the AK-47.

Now many would say “attribution is hard.” Yes, tracking down criminals is hard work. Ask any investigator in any major police department. Criminal investigations are hard. International criminal investigations are harder. But, as we’ve seen in the industry, they are not impossible. The community of “White Hat” investigators working in private industry and law enforcement groups throughout the world have proven that international investigations that lead to arrest and prosecution will work. The first step is for all organizations to focus on the right problem - the human criminal. The next step is to report the crime to through their channels and try to investigate. To do this, the organizations needs to have information for which investigators can build a chain of evidence that can be used to “backtrace” the attack. Parts of this SP Security checklist is designed to help with that backtracing.

**Three Macro Threat Vectors**

Thanks to Mr. Snowden, everything is now on the table for the types of threats organizations need to build risk models to protect against. There are three macro security-risk vectors that an organization needs to consider. Nation state risk - cyber-criminal risk, and P3 Risk. All organizations need to be mindful of all three
risk. Each has their own characteristics and behaviors that will apply to different organizations. All three are permanent threats vectors - with little chance that things will get better in the future. In other words, all three security threat vectors are force of nature that will impact a business sometime in the future.

**Nation State Threats**

All of the Internet is a battlespace for nation-state actors. What does “battlespace” mean to a company? It means that all assets which are connected to the Net are legitimate targets during any nation-state conflict. The national security agencies for many countries have dedicated cyber-warfare and espionage teams whose complete focus is a mission in which they prepare for the attack and defense of their nation. No one can fault these teams for fulfilling their mission. The problem today is that we have little to no international guidelines to govern what is acceptable during the times between conflicts. Given this, we have nation state groups who will penetrate and prepare attacks in networks throughout the world - preparing for the day when it may be needed. If in doubt, review all the materials from Edward Snowden archives (https://cjfe.org/snowden). Extrapolate that techniques and approaches to a multitude of countries throughout the world.

Many businesses would dismiss nation state threats as something that “is beyond” their capabilities. This is a flawed risk assessment. What is meant is that a company is giving up and allowing a nation-state organization to colocate arms and munitions on their company facilities. Not many companies would agree to allow any nation state actor to use their resources in this way in the physical world. The same is true on the Internet. The essential advice from experience is not to give up. There are simple techniques that can be used to disrupt the operations of nation-state actors on trying to impolite inside your operations. The checklists in part 2 have actions that will spot nation state actors as they try to impact and embed inside your network.

**Cyber-Criminal Threats**

Crime on the Internet is a persistent threat. Cyber-crime will be with us until there is sufficient international legal infrastructure to push back against the crime. Until then, the criminal threats will be global, wide-ranging, innovative, and cyclical. The crime cycles are impacted by three factors - new crime business model, ever-evolving criminal toolkits and the local economic factors. We know there will always be places in the world where the local economy is weak and people are looking for a means to make money. International cyber-crime is attractive given the perception that they cannot get caught. These criminals tap into a specialize criminal “toolkit” eco-system that build new tools that are in continues innovation.
cycles. As the white hat community knocks down existing tools, the criminal toolkit specialist innovate with new features that bypass the defenses and countermeasure. Often these criminal will interact with others inside their country and “criminal peers” in other parts of the world. This dialog leads to criminal innovations which subject individuals and organizations to new waves of victimization.

While the prospects are scary, there are ways to push back against the cyber-criminal. The first steps are to use low-cost techniques that make it harder for the organization to get victimized. The core function of this SP Security checklist approach is to cover all these low-cost items and get them deployed first.

**Political, Patriotic, Protestors Threats (P3)**

1991 was a security watershed on the Internet. It was the first time that Denial of Service (DOS) attacks were used as part of a Patriotic and Political retaliation. Yugoslavia was breaking up. Passions were extreme. These did not stop in the physical world, with all sides launching attacks against each other on the emerging Internet and Bulletin Board Systems (FidoNet, UUCP, etc.). This market the emergence of the P3 threat. P3 is the threat from actors who are politically motivated, patriotic to their cause, and passionate about a cause. They are different from the nation state and cyber-criminal threat. Nation-state actors have Generals 'in charge' of the troops. There are Generals who command the groups who are then governed by their government. Cyber-Criminals do nothing for free. They are all about making money by victimizing others. If there is no money, then they move on to other activities where they can make money. They have no interest in “taking out” the Internet if "taking out the Internet" means disrupting the criminal cash flow. The P3 threat is different. These are actors who have no one “in charge.” Their objective is to their cause, their belief, their loyalties. In some ways, they are the most dangerous of the three vectors in that they will use trash and burn techniques if they believe it will meet their personal objective.

Some will want to group the P3 threat with the cyber-criminals or the nation state actors. This is a mistake. The three groupings are particular to the “governors” behind the threat. Often the P3 threat does not have any governing factors push back against the individuals - making their attacks more damaging to the business. Again, the techniques listed in this first SP Security checklist are designed to help organizations prepare for all threat vectors - including the P3 threat vector.
How to you mitigate risk? Prepare, Plan, Drill, and Practice

Security is not something you can read and in a book, white paper, or presentation and then hope you know what you are doing when the S@#$ hits the fan. Ask a firefighter what would happen if they sat around every day and looked at logs. Yes, people will die. Preparing for a security threat against your company and your customers is no different that a fire department preparing for an emergency. If an organization truly wishes to mitigate risk, then they must invest the time for their team to prepare, plan, drill, and practice security. Focused time is the #1 factor between an organization that is ready for an attack and one that has expensive tools which no one knows how to used.
There is good news. Preparing for security incidents on the Internet does not have to be hard. There is always someone knocking on the walls of the network’s defense. This means that the network and security teams can use this known "knocking" to practice. They can do the investigative tracebacks. They can active defensive tools. They can work with their peers to find the malware and botnets, the command & control, and explore ways to disrupt the “criminal’s toolkit.”

In classes, I ask my students to look in their spam folders. There will always is spam linked to spear phishing (or just phishing). We use these phishing emails to start an investigative backtrace. Students start learning the tools, to build a profile. We then use this profile information to explore what the tools on the network can tell us about what is happening. It is an interesting and informative journey as operators see how much is available to them without spending enormous cost to some security firm for “threat intelligence.” The key is time. Time consistently allocated to practice and improve the skills before there is a crisis attack.

If an organization is unwilling to allocate the time with low cost and open source security tools, then there is no point spending millions of dollars on all sorts of security devices which would never get used. You can spend a tremendous amount of money in a “state of the art” fire engine, but the fire engine is just a “shiny object of ego.” If you do not allocate time to train, practice, and improve the skills of the people who will use that fire engine, then the “investment” is a waste of time.

The number one test operators who read thought this checklist can do to see if their executive management is serious about security is ask for dedicated time to practice. One day out of five should be a “security day.” If the leadership of an organization dismisses this allocation of time, then you would know what they really think of the force of nature that is today’s cyber-security environment.
Don't make Excuses for Your Own Security ‘In-Action’

Executives are not the only people making “security excuses.” In fact, the engineers and operators in planning, deployment, product management, operations, customer support, IT, and many other parts of a service provider ignore the threats to their network and their customers. The excuses are always interesting. Here are some examples:

1. **“LaLaLa I cannot hear you,” if I ignore you may be you will go away.** The data is real. Security threats on the Internet in the telecommunications world are a force of nature. Someday they will impact your network. Ignoring the threat will not make it go away.

2. **It is someone else's problem.** Finger pointing at some other group is what the bad guys leverage for their gain. They know that organizational finger pointing leads to complacency - which then opens exploitable holes. Everyone in an organizations has responsibilities to the customers, the shareholders, and to each other. These responsibilities include the safety and security of a the organization - including cyber-security risk.

3. **I need to wait for someone to tell me what to do.** Nonsense! There is enough materials, tutorials, guides, best common practices, and other materials freely available on the Internet for anyone who has a desire to find something they can do to improve the security of their organization. This checklist is pulling together materials that is not new. It is just a new way to focus action.

4. **No one has been killed ..... Yet.** Some is having problems with their heart. They trigger their life alert system to call for help. The problem is that the network is choked up with a DDOS attack. The Service Provider figures they can ride out the attack. The person dies. Who is at fault? Risk is about consequences. Consequences impact lives. Liability will be something that be a shock to the telecoms world. Everyone wanted convergence, now we have it. That means service providers must accept the liability for the lives they impact when their services are not available - even if that availability is impacted from attacks by people on the other side of the planet.

5. **I need more training?** Type “Service Provider Security Bootcamp” in any search engine. Security training is something I hear from service providers all the time. We have enough training on-line that to get anyone started. We have communities of peers in the network operations forums (like MYNOG, SGNOG,
NANOG, etc) who would willingly help each other. Service Provider Security is a collective responsibility. The more networks that deploy the fundamentals, the better for everyone.

6. **We cannot afford all the security equipment?** Notice in the checklist that the key element that requires cost are services, disk, and ports for the storage and analytics capacity. We know form experience that deployment of the open source, top best common practices, and practical tools build significant resilience and capacity inside of an operator. In fact, it has always been a recommendation to have the team deploy the open source tools first. This provides the foundation experience and executive commitment to find the right tools for their organization’s security needs.

7. **Security is the Vendor’s Responsibility!** I hear this from operators who want to “blame the vendor.” Before pointing fingers at the vendor, walk through the “Vendor Security Checklist” (see https://www.linkedin.com/pulse/20140727141634-7430592-questions-to-ask-vendors-to-gauge-their-commitment-to-secure-products). Yes, vendors are partners in the security of your operations and services. But, it is up to the operator to push the vendor. The Vendor Security Checklist was created specifically to be a conversation tool to improve the security of the network.

===============================

➡️ Barry Greene is Business Development Executive ★ Internet Technologist ★ 25 Year Veteran of Internet Security ★ Emerging Technology Mentor ★ Advisor to Innovative Startups ★ Internet in Asia Expert

➡️ Barry connects to peers, colleagues and aspiring talent via Linkedin (www.linkedin.com/in/barryrgreene/). You can also follow on Barry on Twitter (@BarryRGreene) or his blogs on Senki (www.senki.org).