### Preparing for a Data Breach

### Cybersecurity Factors Credit Unions & Community Banks Should Consider

## Introduction

As a managed cyber-security services platform NetWatcher understands that the process of security always comes before the tools like NetWatcher that are used to monitor the security. Given each industry is so different in regards to the process of compliance we have written eBooks that hopefully can guide you through the basics of understanding the industry from a 100k foot view. This eBook is for the Community Banking and Credit Union industries—both unique but suffer from some of the same pains (being able to afford to do cyber security right—Something NetWatcher’s low cost / high value managed service understands).

So let’s begin, what are the regulatory authorities saying about cyber security in this industry:

*“...recent cyber-attacks have targeted interbank messaging and wholesale payment functions at financial institutions to originate unauthorized transactions. These unauthorized transactions may subject a bank that originates such transactions to losses and compliance risk” --* [*FFIEC*](https://www.ffiec.gov/press/pr060716.htm)

*“Cyber-attacks against financial institutions to extort payment in return for the release of sensitive information are increasing. Financial institutions should address this threat by conducting ongoing cybersecurity risk assessments and monitoring of controls and information systems. In addition, financial institutions should have effective business continuity plans to respond to this type of cyber-attack to ensure resiliency of operations.” -* [*FFIEC*](https://www.ffiec.gov/press/pr110315.htm)

When Smaller Community banks and Credit Unions read such messages they shudder as they don’t have the resources of J.P. Morgan to invest in cyber security (more on J.P. Morgan’s $500 million a year investment on cyber-security [here](http://www.wsj.com/articles/j-p-morgan-to-accelerate-timeline-for-cybersecurity-spending-boost-1438641746)). While they may not offer as rich a target as the nation’s biggest institutions, small banks and credit unions know that they are still attractive targets for cyberattacks and for those seeking a point of entry into the financial system.

Community banks and credit unions also bear a significant burden as they incur steep losses in order to reestablish customer and member safety after a data breach occurs, whether online or otherwise. A February 2015 NAFCU [**survey**](http://www.nafcu.org/News/2015_News/February/ECUM___226K__1_600_hours_spent_per_CU_on_data_breaches/) reports credit unions, on average, spent $136,000 on data security measures and $226,000 in costs associated with merchant data breaches in 2014.

Every community banking and credit union association is talking about cyber security and making recommendations, however the reality is that these entities just can’t afford to hire security analysts (they couldn’t find them if they could afford them –more here) and they cannot afford expensive solutions from IBM, HP and FireEye that run in the hundreds of thousands of dollars..

***Sidebar***: On July 14, 2015 at the American Bankers Association Summer Leadership meeting ([remarks found here](https://www.treasury.gov/press-center/press-releases/Pages/jl0112.aspx)), Deputy Secretary of the Treasury Sarah Bloom Raskin addressed issues related to cybersecurity and cyber-resiliency. Recognizing the unique threat cyber-attacks pose to the banking system, the Treasury Department has made ensuring cybersecurity a high priority. Deputy Secretary Raskin noted that the litany of cyber-risks could be "uniquely devastating" to the financial sector, which is heavily invested in e-commerce and e-banking.

Based on the assessment of the unique risks to the financial sector, Deputy Secretary Raskin posed 10 questions designed to better equip the banking leaders in their efforts to oversee cybersecurity efforts at their respective institutions:

1. Does our bank embed cybersecurity into our governance, control and risk management systems?
2. Have we remained vigilant about systematically identifying our key assets, those that provide high-value targets for malicious cyber actors?
3. Have we tailored our security controls to the specific cyber risks presented by each key network, system or set of sensitive data?
4. How do we prioritize the implementation of enhanced controls around key networks, systems and sensitive data?
5. Have we reviewed the FFIEC Cybersecurity Assessment Tool and appropriately incorporated it into our approach to cyber-risk management?
6. Have we designated specific professionals to handle our cybersecurity strategy and provided them with the authority, resources and access they need to effectively perform their work?
7. Have we trained our personnel on our cybersecurity policies?
8. How do we ensure that our insurance coverage matches our cyber-related risks?
9. Does our cyber-risk insurance impose "minimum required practices," which may lead to denial of coverage if not followed?
10. Do we practice basic cyber hygiene?  
    * Do we require multi-factor authentication before allowing access to our networks, systems and data?
    * Have we restricted special, high-level access to only those who need it?
    * Are we doing regular maintenance and consistently patching our software?
    * Are we effectively scanning our systems for malicious activity?

## Case Studies

You don’t want to end up like one of the following. Reputation damage alone would take a significant toll on your organization let alone the cost of lawyers, forensics, remediation, regulatory fines etc…

|  |  |
| --- | --- |
| **Financial Institution** | **What Happened** |
| Pentagon Federal Credit Union | A laptop was found to be infected with malware. A PenFed current and former employees, beneficiaries, current and former members and joint owners may have had their names, Social Security numbers, addresses, credit and debit card numbers, and PenFed account numbers exposed. The breach affected 674 New Hampshire residents and an unknown number of people nationwide. |
| Five County Credit Union | Five County decided to send 3,000 credit and debit cards to customers after discovering a breach that affected a third party. After some customers noticed suspicious transactions on their debit cards about 2,500 debit cards were reissued and 500 Visa credit cards were reissued. The organization that experienced the breach and the number of customers affected were not reported. |
| Associated Credit Union | About 100 Associated Credit Union members have experienced fraudulent checking account charges. A breach of check and ATM card information may have been caused by a breach of Associated Credit's processing company. The customer information was used to make fake cards and the cards were sold throughout the country. |
| Abilene Telco Federal Credit Union | A hacker or hackers were able to access an Abilene Telco Federal Credit Union employee's computer. The Bank's online account with Experian was then used to download the credit reports of 847 people. Social Security numbers, dates of birth and detailed financial data were exposed. |
| Rockland Federal Credit Union | Rockland Federal Credit Union sent customers new debit cards with new PINs as a result of a merchant who discovered a breach in their computer system. |
| Monadnock Community Bank | At least 13 New Hampshire residents and an unknown number of other U.S. customers were affected by a breach of Monadnock's card processor. Customer debit card numbers, expiration dates, CVC and PIN offsets may have been exposed. |

From <http://www.privacyrights.org/data-breach>

## Organizations with Oversight

Financial institutions in general have a great deal of oversight at both the Federal and the State level. When it comes to cyber security protection there are a few organizations that stand out for both community banks and credit unions.

The Federal organizations that have a say in the way community banks and credit unions conduct themselves are as follows:

* **Federal Financial Institutions Examination Council (**[FFIEC](https://www.ffiec.gov/cybersecurity.htm)) - The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System ([FRB](http://www.federalreserve.gov/)), the Federal Deposit Insurance Corporation ([FDIC](http://www.fdic.gov/)), the National Credit Union Administration ([NCUA](http://www.ncua.gov/)), the Office of the Comptroller of the Currency ([OCC](http://www.occ.treas.gov/)), and the Consumer Financial Protection Bureau ([CFPB](http://www.consumerfinance.gov/)), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee ([SLC](https://www.ffiec.gov/slc.htm)) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors ([CSBS](http://www.csbs.org/)), the American Council of State Savings Supervisors ([ACSSS](http://www.acsss.org/)), and the National Association of State Credit Union Supervisors ([NASCUS](http://www.nascus.org/)).
* **Consumer Financial Protection** Bureau ([CFPB](http://www.consumerfinance.gov/)) - a U.S. government agency that makes sure banks, lenders, and other financial companies treat customers fairly.
* **Federal Trade Commission** ([FTC](https://www.ftc.gov/datasecurity)) **-** Companies with personal information should take steps to safeguard their data. Otherwise, that information could fall into the wrong hands, resulting in fraud and other harm. The FTC promotes data security in the private sector through civil law enforcement; education; policy initiatives; and recommendations to Congress to enact legislation in this area. The touchstone of the FTC’s approach to data security is reasonableness: a company’s data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.

Credit unions have one additional group:

* **National Credit Union Association** ([NCUA](https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/resource-centers/cyber-security.aspx)) - The mission of the NCUA is to provide, through regulation and supervision, a safe and sound credit union system, which promotes confidence in the national system of cooperative credit. Learn more about NCUA’s mission, culture, values and how we ensure millions of Americans can safely and confidently use credit unions for their financial needs.

## Helpful Organizations

There are also several organizations that provide a helping hand to both community banks and credit unions. This is not an exhaustive list by any means:

* [CBANC](https://www.cbancnetwork.com/) - The professional network for bank and credit union professionals, empowering them to collaborate, share information and lead the evolution of community banking.
* **National Association of Federal Credit Unions** ([NAFCU](http://www.nafcu.org/)) - a direct membership association for federally insured credit unions committed to representing, assisting, educating and informing their member credit unions to help them grow, and help grow the credit union industry.
* **Financial Services - Information Sharing and Analysis Center** ([FS-ISAC](http://www.fsisac.com/)) – An industry forum for collaboration on critical security threats facing the global financial services sector.

## Regulatory Compliance & Cyber Security

The Policy that primarily drives all cyber security with financial institutions at the Federal level is the Gramm-Leach-Bliley Safeguards rule. These laws impact both community banks and credit unions.

* The Gramm–Leach–Bliley Act – ([for details](https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act)  [6801](https://www.law.cornell.edu/uscode/text/15/6801)–[6809](https://www.law.cornell.edu/uscode/text/15/6809)) GLBA requires financial institutions (companies that offer consumers financial products or services like loans, financial or investment advice, or insurance) to explain their information-sharing practices to their customers and to safeguard sensitive data. The Act contains three elements (Privacy Rule, Safeguards Rule and Pretexting Protection) regarding the privacy of information, of which businesses, primarily "financial institutions," need to be aware – for this paper we will cover the GLBA Safeguards Rule ([More from the FTC](https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying)).

The Safeguards Rule requires an institution to develop, implement, and maintain a comprehensive information security program that is written, contains administrative, technical and physical safeguards, is “appropriate” to the institution’s size and complexity, as well as the nature and scope of its activities, and is appropriate to the sensitivity of the customer information at issue.

The FTC requires ([more here](https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying)) companies to conduct a thorough risk assessment and address such risks to customer information in all areas of their operation, including administrative, technical, and physical safeguards. As part of the risk assessment, the Safeguards Rule requires an institution to:

* Designate someone to coordinate the information security program;
* Perform a thorough risk assessment and identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

1. Employee Training and Management. A costs of compliance is related to employee training and management. A financial institution’s risk assessment should:
   * Check employee references and perform background checks;
   * Require employees to sign a confidentiality agreement;
   * Limit employee access to sensitive customer information;
   * Use password-activated screen savers to lock employee computers;
   * Encrypt customer files on laptops and other computers in case of theft;
   * Impose disciplinary measures for security policy violations;
   * Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names. The FTC noted in one of its publications that “the success of your information security plan depends largely upon the employees who implement it.”

2. Information Systems. The Safeguards Rule requires a financial institution to assess its information systems, including network and software design, as well as information processing, storage, transmission, and disposal. A financial institution’s written information security plan should include both technology concerns and the physical storage and destruction of nonpublic personal information. For example:

* + Know where sensitive customer information is stored and stored securely;
  + Ensure that the computer or server is accessible only by using a “strong” password and is kept in a physically secure area;
  + Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area;
  + Take affirmative steps to secure transmission of customer information;
  + Encrypt customer data if it is necessary for you to transmit such information by email or Internet;
  + If you collect information online directly from customers, secure the data transmission automatically;
  + Dispose of customer information consistent with the FTC’s Disposal Rule.

3. Plan for System Attacks. The Safeguards Rule requires a financial institution to detect, prevent, and respond to attacks, intrusions, or other system failures. A financial institution must remain constantly vigilant, and employ the latest security measures and technology in order to adequately protect its network. The FTC Guidance report suggests that financial institutions:

* + Monitor the websites of software vendors and relevant industry publications for news about emerging threats and available defenses;
  + Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
  + Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
  + Take affirmative steps to preserve the security, confidentiality, and integrity of customer information and consider notifying consumers, law enforcement, and credit bureaus in the event of a security breach;
  + Oversee service providers by ensuring that they are able to take appropriate security precautions and in fact do so;
  + Update the security program as necessary in response to frequent monitoring and material changes in the business.

C. Implementing and Maintaining the Information Security Program.

The Safeguards Rule requires an institution to design and implement information safeguards to control the risks identified and regularly test and monitor the effectiveness of the information security program’s key controls, systems, and procedures. This duty also includes overseeing third-party service providers by taking reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards and requiring the service providers to contractually agree to implement and maintain such controls. The Safeguards Rule requires a financial institution to evaluate and adjust its information security program in response to its system test results or in response to any changes in its operations or business circumstances.

**Sidebar**: An important factor for institutions to consider is the potential discoverability of risk assessments. Talk to an experienced cyber security attorney about avoiding potential discovery issues and have any risk assessments covered by the attorney-client or the attorney work-product privilege. The rules regarding these privileges are state specific.

### Credit Unions

* NCUA’s rules and regulations
* **Develop a Written Information Security Program** See, [12 CFR 748 App. A](http://www.ecfr.gov/cgi-bin/text-idx?SID=eca9d5b54c313d6cc801843940930c2e&mc=true&node=ap12.7.748_12.a&rgn=div9).  [Section 748.0](http://www.ecfr.gov/cgi-bin/text-idx?SID=125f4524cc913228d0e9717444cdd0b0&mc=true&node=se12.7.748_10&rgn=div8) of NCUA’s rules and regulations requires each federally insured credit union to have a written security program within 90 days of insurance by the NCUSIF.  [Appendix A to Part 748](http://www.ecfr.gov/cgi-bin/text-idx?SID=eca9d5b54c313d6cc801843940930c2e&mc=true&node=ap12.7.748_12.a&rgn=div9) sets forth guidelines for safeguarding member information.  In general, the guidance requires credit unions to have documented policies and procedures that implement and address the credit union’s information security program.
* **Develop a Cybersecurity Incident Response Program.**Incident response programs address the action steps a credit union should take in the event of a data breach.  The regulatory requirements for a credit union’s incident response program are contained in [Appendix B to Part 748](http://www.ecfr.gov/cgi-bin/text-idx?SID=eca9d5b54c313d6cc801843940930c2e&mc=true&node=ap12.7.748_12.b&rgn=div9).  [Appendix B](http://www.ecfr.gov/cgi-bin/text-idx?SID=eca9d5b54c313d6cc801843940930c2e&mc=true&node=ap12.7.748_12.b&rgn=div9) provides guidance on response programs for unauthorized access to member information, including standards for providing members with timely notice of unauthorized access or use of member information.  It is also good practice to include the when, and what type of, recourse will be offered to victims of a breach.

## Tools

* **FFIEC Cyber Assessment Tool (**<https://www.ffiec.gov/cyberassessmenttool.htm>)
* **Conference of State Bank Supervisors Executive Leadership of Cybersecurity Resource Guide** ([found here](https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf))
* **The FDIC** **Community Bank Cyber Exercise** ([found here](https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html#two)) – Created to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions.
* **FFIEC Handbook’s Section on Information Security** ([found here](http://ithandbook.ffiec.gov/it-booklets/information-security.aspx))
* **FDIC Framework for Cybersecurity** ([found here](https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/SI_Winter2015.pdf)) - The article addresses some common cyber-attack strategies, the critical components of information security programs (corporate governance, threat intelligence, security awareness training, and patch-management programs), and actions taken by federal bank regulators to respond to cybersecurity threats. The article stresses that everyone within a financial institution, from entry-level staff to the board of directors, is responsible for prioritizing cybersecurity. The article includes information about several resources available to help educate and inform employees and directors on cybersecurity.
* **NIST Cyber Security Framework** ([found here](http://www.nist.gov/cyberframework/))
* **Conference of State Bank Supervisors Executive Leadership of Cybersecurity Resource** Guide ([found here](http://www.csbs.org/cybersecurity)) - provide community bank CEOs and executive management with a “non-technical, easy-to-read resource on cybersecurity.” The CSBS Guide is intended to “put in one document industry recognized standards for cyber security, best practices currently used within the financial services industry, and an organizational approach used by the NIST.
* **FDIC - A Bank Customer’s Guide to Cyber Security** ([found here](https://www.adamscommunity.com/wp-content/uploads/2016/03/FDIC-Customers-Guide-to-Cybersecurity.pdf)) – An explanation of What Consumers Can Do ... and What Banks and Regulators Are Doing ... to Help Prevent Online Fraud and Theft

## Legislation to Follow

* H.R. 2205, the Data Security Act of 2015 – ([more](https://www.govtrack.us/congress/bills/114/hr2205/summary))
* New York Department of Financial Services Sets Forth Extensive Cybersecurity Regulatory Framework – ([more](https://www.dataprivacymonitor.com/cybersecurity/new-york-department-of-financial-services-sets-forth-extensive-cybersecurity-regulatory-framework-proposal/))

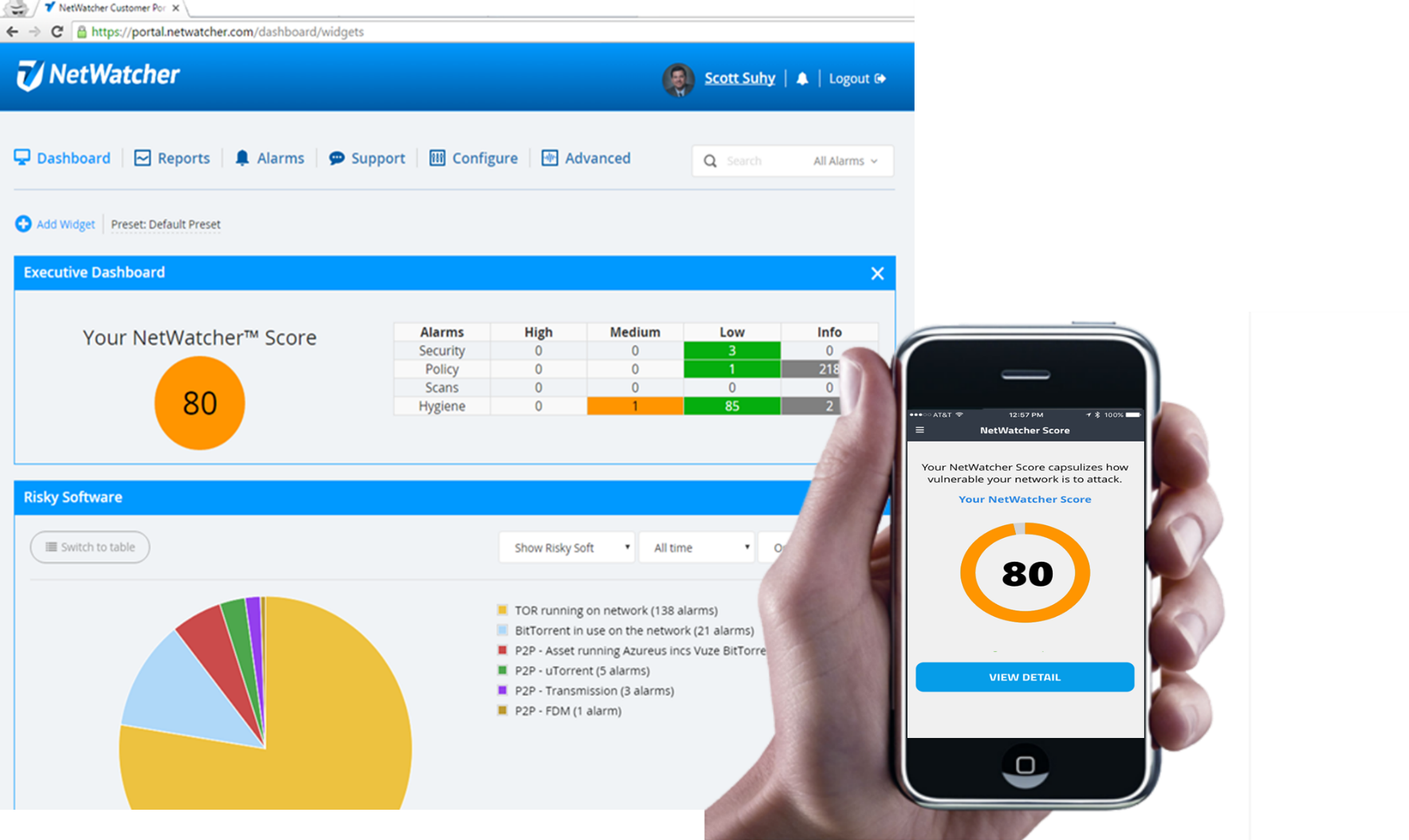
## Using NetWatcher for Situational Awareness of your Networks Security

### What is NetWatcher?

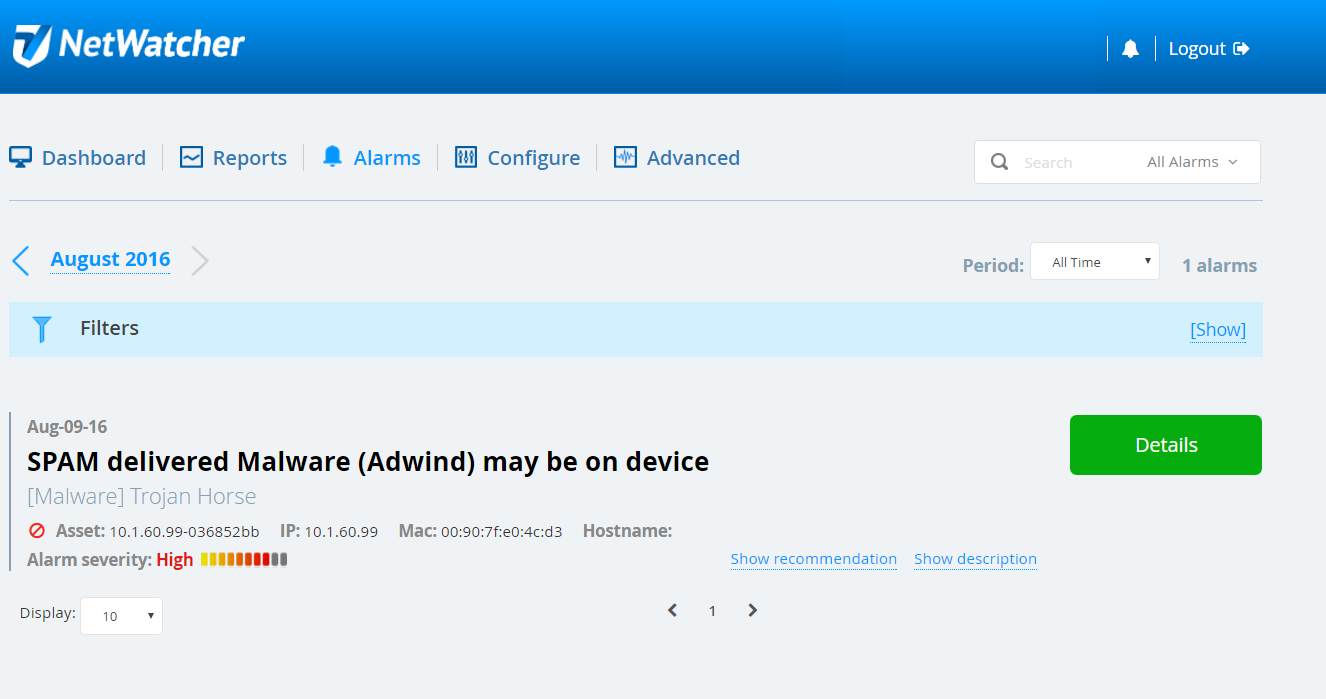
NetWatcher is a Security-as-a-Service platform that enables customers to have a cost-eﬀective 24 x 7 security service monitoring their networks for vulnerabilities and exploits. Many government and industry compliance requirements, and security best practices, outline the need for continuous monitoring, intrusion detection, active scanning, log monitoring, net-ﬂow analysis, event management and end point integration. NetWatcher enables customers to immediately deploy these services and take advantage of a fully-staﬀed Security Operations Center (SOC). This means superior security that is easy to use, accurate and affordable.

### Your Network Security Risk Score

NetWatcher is a 24x7 Security-as-a-Service platform designed to continually analyzes data about the state of a corporate network. One of NetWatcher’s powerful features is its ability to devise a single numerical score that gives a quick sense of security risk.



### Monitoring for Exploits



### Monitoring your Security Hygiene

What is security hygiene? It is essentially how well you are managing your network security and the activities your employees are doing on a day to day basis that may compromise the security of your network, opening your company/agency up to exploit.

#### Employees Activities

Most exploits occur due to non-malicious users letting bad actors into the enterprise unknowingly… The security industry calls this the *Unintentional Insider Threat* problem (more [here](http://www.sei.cmu.edu/reports/13tn022.pdf)).

Some examples are:

* Employees running old vulnerable software such as Flash or Java versions that are littered with exploitable problems. ([here](http://www.bankinfosecurity.com/blogs/nuke-old-java-ftc-tells-oracle-p-2014) is a good article on what the FTC thinks of Java). [Here](http://bits.blogs.nytimes.com/2015/08/03/hackers-exploit-flash-vulnerability-in-yahoo-ads/?_r=0) is another example how an old version of Flash might exploit the enterprise…
* Employees running risky software such as BitTorrent and Tor.
* Employees sending Personally Identifiable Information (PII) data such as passwords or credit card numbers over the internet in clear text.
* Employees going to nefarious websites.
* Employees clicking on phishing messages.

|  |  |
| --- | --- |
| As you can see from the latest 451 Research study User Behavior (14%) is the leading internal IT security pain point. | https://www.451alliance.com/Portals/5/2015reports/121615_security_report/7_pain_points.gif |

|  |  |
| --- | --- |
| With NetWatcher each week by default (configurable) all users get an email with the security posture of the network. The email has the widget, seen in figure 1, that provides you a score (out of 100, normalized over the number of assets on the network), and how many violations have resulted in open alarms, of various priorities, over the last 2 weeks. Executives like this email because it can tell them very quickly if their score is going up or down and what is driving the score in one direction or the other. They can also click on each item in the grid to see the exact issue and what user/asset on the network is causing the potential risk. |  |

|  |  |
| --- | --- |
| If you navigate over to the NetWatcher dashboard you can also install many widgets like the two you see in figure 2 related to the number of users running risky software or vulnerable software. |  |

It’s important to deal with these hygiene issues as they arise. You can either:

1. Upgrade the software if necessary
2. Remove the software if it is too risky
3. Train the user on why the activity or software they are using exposes them and the company to exploit
4. Update employee policy documents to include what a user can and cannot do on the network
5. Block the software at the firewall/router &/or use web gateways to block the users for visiting bad sites &/or use email phishing services to force users to be smart about what they are clicking

#### Network Security

|  |  |
| --- | --- |
| You also want to keep an eye on what’s getting through your firewall, especially from countries like Iran, China and Russia. With NetWatcher, one of the widgets we provide is to show you all the countries that have triggered anomalous events once they made it through the firewall. If you click on any country in the widget in figure 3 you will be taken to the corresponding events and can review all the detail including downloading the ‘pcap’ or look at related events by the hour or day that occurred on the same asset allowing you to see if the bad actor may be migrating. |  |

|  |  |
| --- | --- |
| You can even set “Trip Wires” to send you an SMS message if one of these events (or any other event for that matter) occurs. For example, here is a SMS trip wire set for any event from China, Iran or Russia. |  |

|  |  |
| --- | --- |
| You also need to keep a close eye on what network “Scanning” is making it through your firewall. NetWatcher provides, widgets for this as well. Here is an example of multiple scans taking place on 2 different corporate assets. |  |

With all of these Security Hygiene items it is up to you to determine if they are normal and safe or do you need to blacklist IP addresses or entire countries at the firewall/router so they can never enter the organization. Do your users do business in those countries? Do your users do business with the organizations that own the IP address of those scanning you? These are just a couple of the questions you will need to ask to determine the steps you need to take to take the action necessary to increase your organizations security posture.

This is just a small glimpse of what you can do with NetWatcher with just the simple IDS/Correlation engine. There are many other things you can do if you install the Secure Information & Event Management system, the End Point technology, the Active Scanning components or the Netflow analysis engine. Have fun!