2014 Entry Form
(Complete one for each entry.)

Fill out the entry name ***exactly*** as you want it listed in the program.

Entry Name Responding to emerging cyber security threats

HFA Idaho Housing and Finance Association

Submission Contact Greg Blake

Phone 208-331-4745 **Email** gregb@ihfa.org

Qualified Entries must be received by **Tuesday, July 1, 2014**.

For more information about Qualified Entries, click here to access the 2014 Entry Rules.

Use this header on the upper right corner of each page.

HFA Idaho Housing

Entry Name Responding to e

Communications	Homeownership	Rental Housing	Special Needs Housing
☐ Annual Report ☐ Promotional Materials and Newsletters ☐ Creative Media	☐ Empowering New Buyers ☐ Home Improvement and Rehabilitation ☐ Encouraging New Production	☐ Multifamily Management ☐ Preservation and Rehabilitation ☐ Encouraging New Production	☐ Combating Homelessness ☐ Housing for Persons with Special Needs
Legislative Advocacy	**Management Innovation**	**Special Achievement**	**Are you providing visual aids?**
☐ State Advocacy ☐ Federal Advocacy	☐ Financial ☐ Human Resources ☐ Operations ■ Technology	☐ Special Achievement	☐ YES ■ NO

Protecting the personal information and identities of your clients and constituents is imperative in today's business environment. A security breach could be costly to your organization and devastating to your brand. Because of this Idaho Housing created and implemented a Cyber Resilience Plan and has taken extensive measures to bolster its security. Ensure that your HFA won't be the next Target…

BACKGROUND

As housing authorities increasing rely on information technology, more and more confidential information exists across the various HFA information systems. This type of information is known as personally identifiable information (PII). The Government Accountability Office (GAO) defines PII as "any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical records, educational, financial and employment information."

IT organizations hire security audit firms to conduct vulnerability and penetration tests. These tests typically use commercial software to port scan, look for incorrect firewall settings, scan for default passwords, check software patching levels, etc. The security firms use software programs with known techniques to test the perimeter of an organization and provide vulnerability assessment reports. Large organizations have security departments with 24/7 monitoring. Small companies, such as HFA's, don't have the luxury of a security department and must rely on firewalls and other measures to protect their organization.

Idaho Housing's vulnerability and penetration testing results score an A+ year after year. We have never had a critical finding reported. We were excellent at ingress filtering, blocking the hackers and protecting the perimeter. But how would our organization hold out if confronted with an advanced persistent threat (APT)? An APT being an expert hacker, cyber-criminal organization, or foreign government organization determined to breach our security and steal our PII.

WHY WE UNDERTOOK THIS PLAN

It was recommended by our audit firm to conduct a 'black box' penetration test using ex-National Security Agency (NSA) and ex-Department of Defense (DoD) white hat hackers. The term 'white hat' refers to ethical hackers used to evaluate an organization's security. The term 'black box' refers to the hackers not having any previous knowledge of our organization who will deploy modern hacking techniques to try to breach our security. Our employees were unaware that a black box test was being conducted, especially the IT department.

Our 'white hat' security company started slow by sending out virus-laden emails that looked like Red Cross donation signups. Fortunately, our employees did not fall for their scam. After a week of trying to breach our security, they were eventually successful by means of a video resume, sent as an email to an employee, with an embedded remote control program.

THE CYBER RESILIENCE PLAN

As a result of the test, the need to craft a plan to protect our computer systems was imperative. We started work on a Cyber Resilience Plan. A Cyber Resilience Plan accepts the risk that an attack may be successful and helps us prepare to mitigate any damage. The plan includes steps to not only protect the network perimeter but to secure the inside of our network with security zones and monitoring. Gone

P.O. Box 7899, (565 W. Myrtle Street), Boise, ID 83707-1899 • Phone (208) 331-4889 • Fax (208) 331-4804

are the days of trusting employees and vendors with elevated privileges on the network. Our number one priority was to secure our computer systems so even dedicated hackers would be unsuccessful.

OUR PLAN
Listed below are some of the steps undertaken in the Cyber Resilience Plan:

Cyber Security Software: In addition to anti-virus software, we purchased and installed cyber security software that includes Data Loss Protection, Data Governance, Security Event Management software, and Sandbox software. These software systems alert our system administrator of unauthorized access attempts on files and folders that contain confidential or personal information.

Remove local domain administrator rights from the computers: Every Microsoft Windows system has a built-in administrator account. If this account is hacked it leads to significant problems because it allows software to be installed by the hacker. The account should be disabled. If you ever need the account for disaster recovery, you can always use the recovery console or boot into safe mode and the account will be enabled.

Remove USB drive access: Hackers love to plant infected USB thumb drives in the parking lots of companies. Employees get out of their cars and see thumb drive on the ground. Their first instinct is to get in the office, turn on their computer, and plug in the thumb drive to see what they found. Fortunately USB drive access can be controlled and disabled using a Windows group policy by the network administrator.

Disable macros in Word and Excel: Hackers have discovered easy ways to inject malware in Word and Excel email attachments. A user opens up an email with a Word or Excel attachment, opens the file, and viola malware is now installed on their system. We disable macros in Word and Excel.

Anti-virus and patch management: Having every computer on the network set up with anti-virus software and current updates is critical to stop common malware attacks through email and web surfing. Malware typically utilizes known vulnerabilities in software that has been fixed by the software authors, but most companies fail to deploy the software patches in a timely manner. We use Windows Update Server (WUS) to make sure all network computers have the latest patches and antivirus signatures.

Remove Java: Java is a programming language that is very easy to develop applications for the internet landscape. In order to run Java programs, a computer must have the version of the virtual Java machine for the operating system or browser. Millions of internet users have installed Java Virtual Machine to run Java applications. Cyber criminals know the popularity of Java and spend a considerable amount of time and resources to exploit the system. We remove Java from any computer not required to use Java for business purposes.

Key-logger protection: When hackers gain control of a single computer, one of their first orders of business is to install a key-logger program to record any keystrokes of the unsuspecting user. They look for accounts and passwords entered by the user to gain access to other systems. Key-logger protection software encrypts and decrypts keystrokes as you type. If a key-logger is installed on your computer, the hackers capture bogus keystroke information.

EMET: Microsoft released a free toolkit call Enhanced Mitigation Experience Toolkit (EMET) that includes important protection for third-party applications installed on a computer. Installing EMET makes it hard for hackers to exploit security vulnerabilities inherent in a Windows operating system. This is absolutely the best defense software for newly released viruses and most malware exploits. We Installed EMET on every computer in the organization and we encourage staff to install this package on their home computers.

Segment the network: If a hacker gains entry to the network, they will scour the network to find entry into areas where the users have privileges. By segmenting the network to areas where a user only has access to the network folders that they need to conduct business will greatly limited damage if their network account is compromised. Creating active directory security groups with limited privileges to the network is required.

Security Awareness Training: Training staff to be aware of exploits and the tricks of the hackers is a necessity of any organization. Teaching staff to be constantly vigilant and not trusting will greatly reduced the probability of getting hacked. We have security awareness training.

Complex password: Password cracking software has become so sophisticated that it only takes a matter of hours for a hacker to derive passwords from users, because the software understands how a majority of people think when they create passwords. Requiring a minimum of 12 characters passphrase, with special characters, is the new norm and makes cracking much more difficult.

Prohibit social media: Eliminate social media access from work computers attached to the network. If an employee wants to check his Facebook or Twitter accounts he can use his own device not attached to the network. Social media sites use JavaScript and are notorious for malware applications disguised as games and other fun posts. We prohibit social media on company computers.

Geo-code website filtering: There should be not be any reason to accept emails from Russia, the Ukraine or other countries that are notorious for malware and cyber-criminal activities. We changed our firewall to block all web activities from country-specific domain registrations.

Port 443 deep packet inspections: In order for computer users to access secure websites, they must use port 443 through the firewall. Advanced firewalls now come with the ability to inspect the port 443 for malicious activity. We replaced our firewall with a newer model that includes deep packet inspection of port 443. This will keep the hackers at bay.

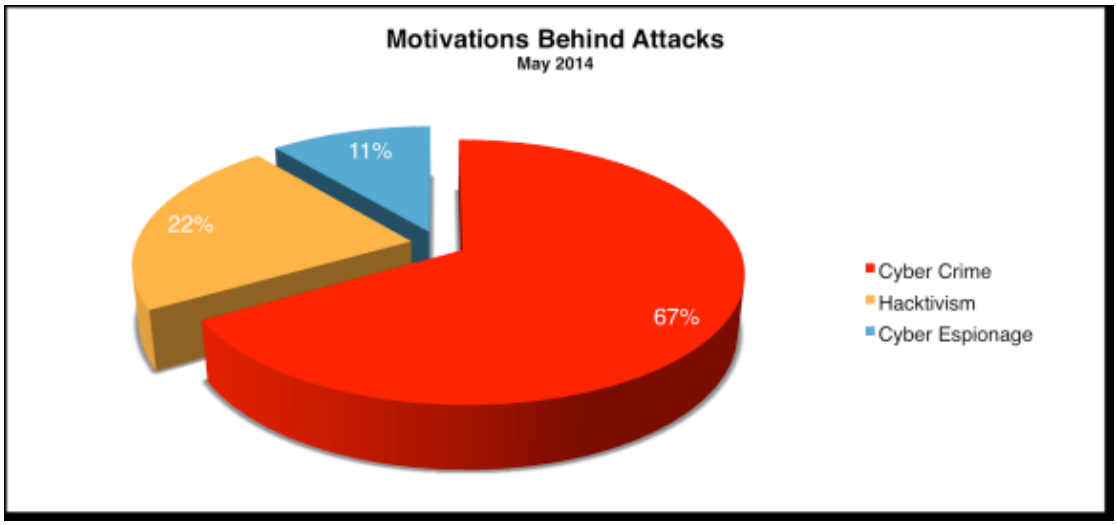
Block internet access in the evenings: There should be no reason to leave internet access available on the network when employees are home. We block internet access during non-work hours and on weekends. Hackers won't be able to access the network during those hours.

Hack your own environments: Set up a program to hack your own network. Pretend you're a hacker and have gained access to an individual's computer. See what you can find and see if you can install software or gain elevated privileges. You will be surprised at how much access typical users have to the network.

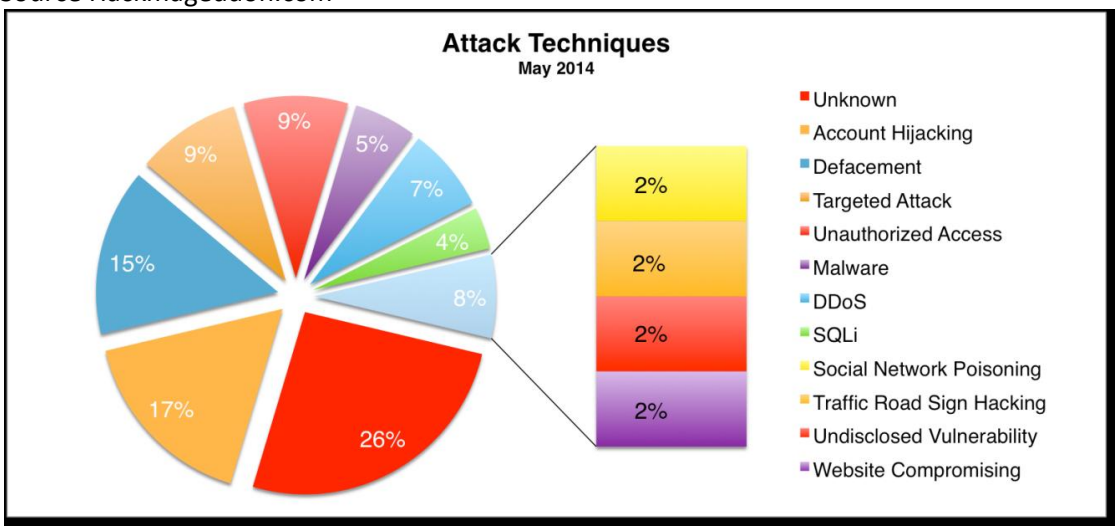
While no system is hacker proof, by implementing these steps our organization has greatly reduced our cyber-security risk profile and helped us pass our stringent SOC 2 audit.

P.O. Box 7899, (565 W. Myrtle Street), Boise, ID 83707-1899 • Phone (208) 331-4889 • Fax (208) 331-4804

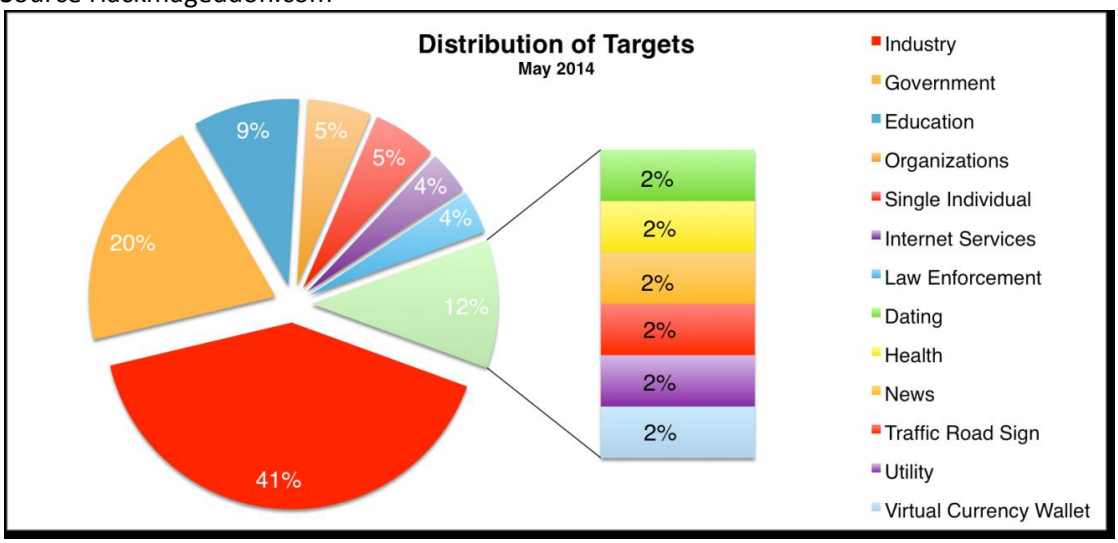
Visual Aids



Source Hackmageddon.com

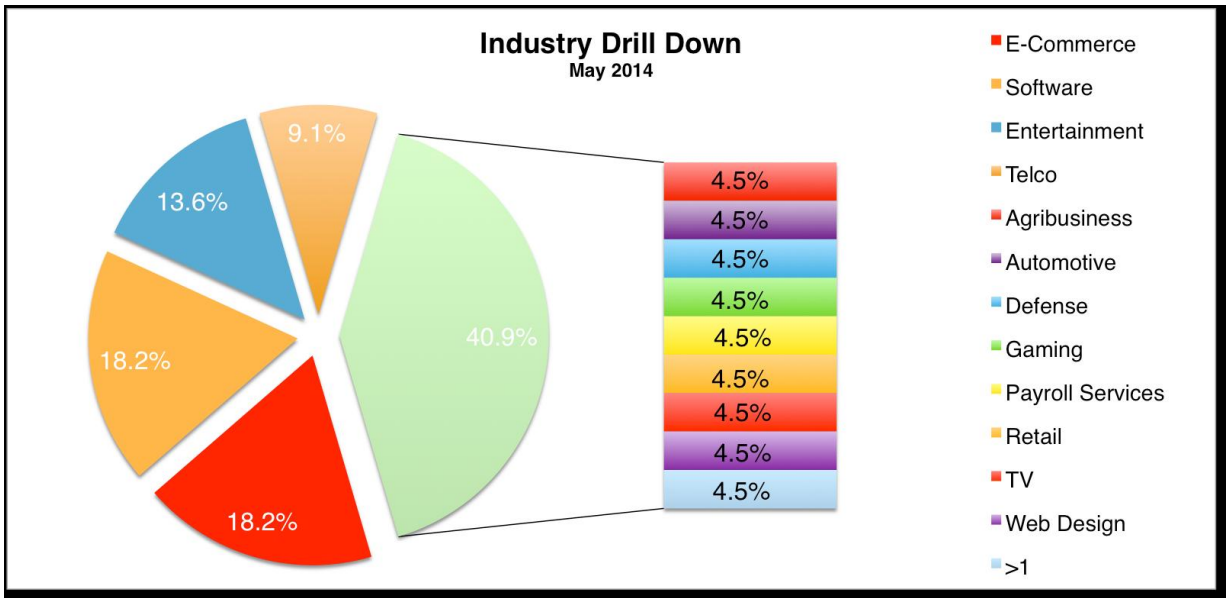


Source Hackmageddon.com

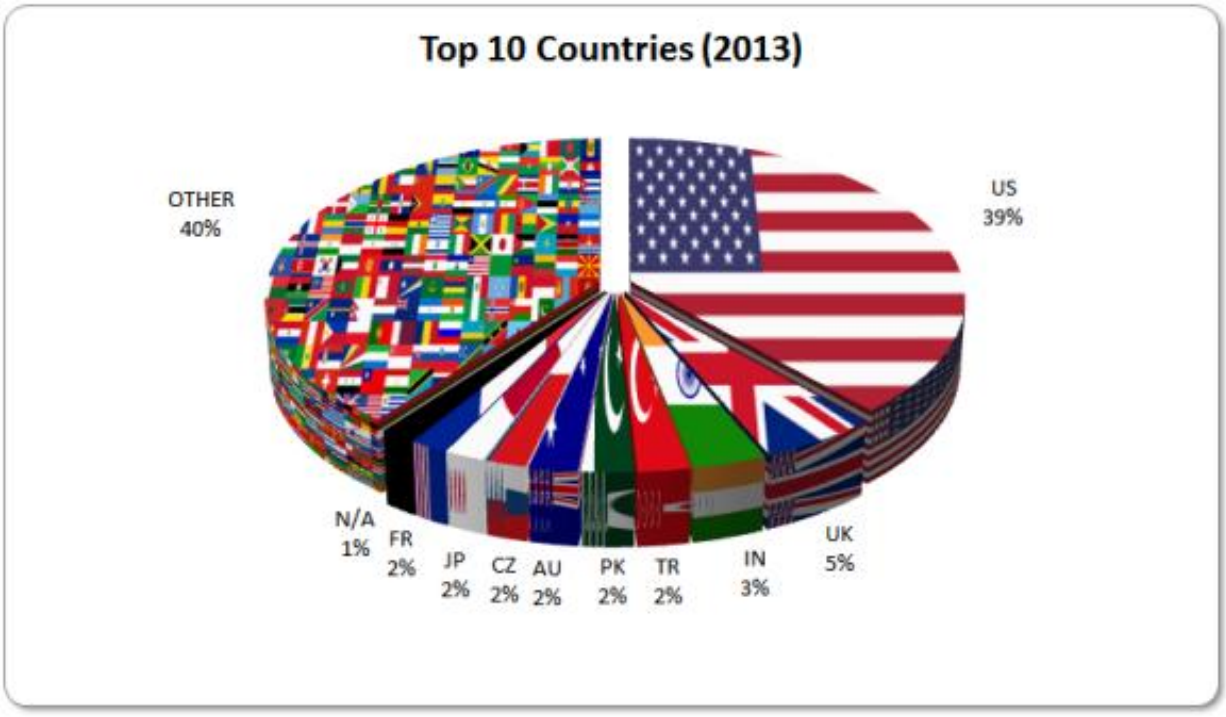


Source Hackmageddon.com

P.O. Box 7899, (565 W. Myrtle Street), Boise, ID 83707-1899 • Phone (208) 331-4889 • Fax (208) 331-4804



Source Hackmageddon.com



Top 10 Counties Attacked: Source Hackmageddon.com

P.O. Box 7899, (565 W. Myrtle Street), Boise, ID 83707-1899 • Phone (208) 331-4889 • Fax (208) 331-4804

Source: ISACA