Maritime Cyber Security White Paper

Safeguarding data through increased awareness

November 2015

GLOBAL SECURITY

Contents

GLOBAL SECURITY

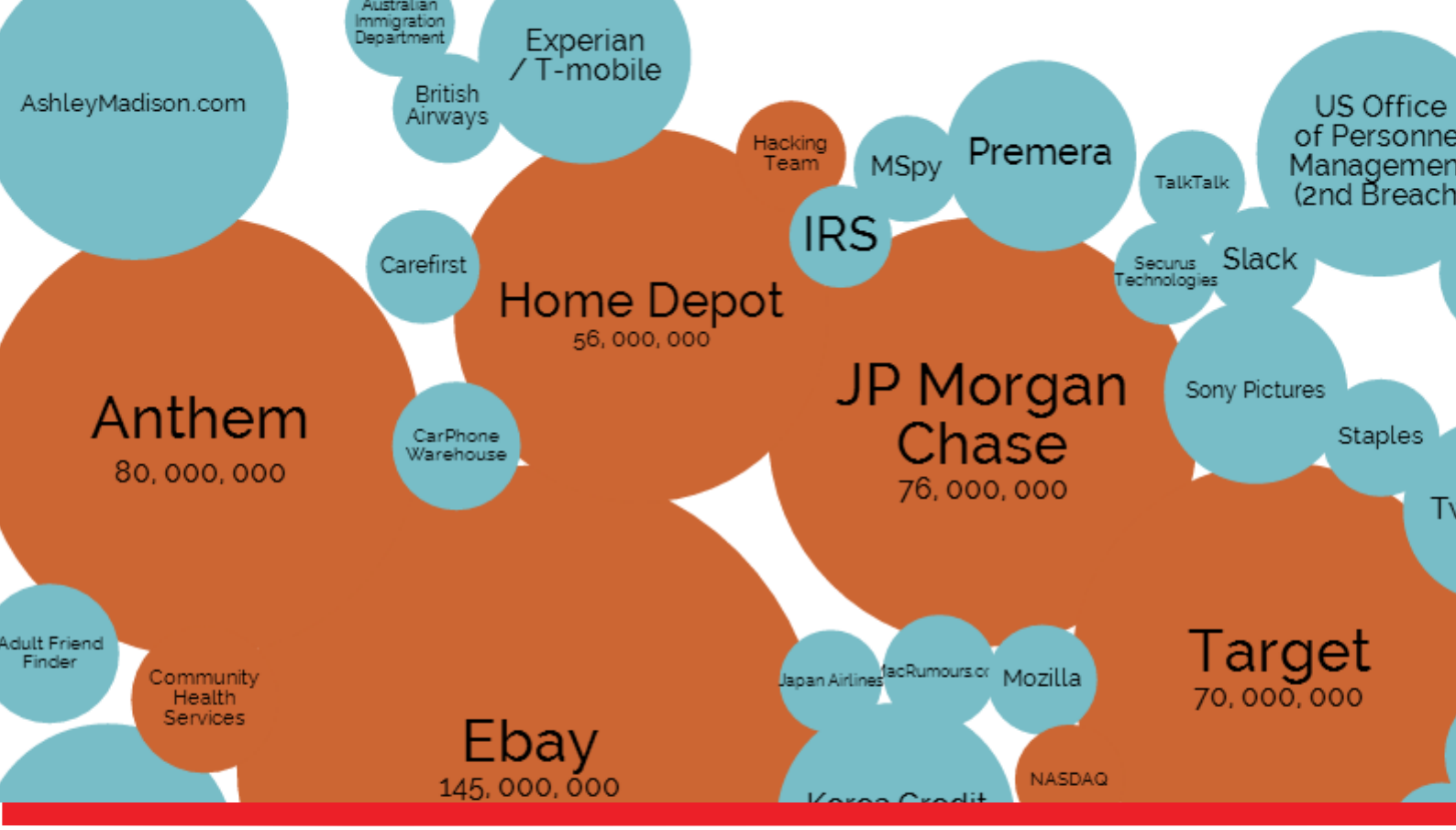
Executive Summary

Advancement in broadband technologies and the move towards ‘Big Data’ and 'Ship Intelligence' could leave the maritime industry vulnerable to cyber-crime unless it develops a better awareness of ICT (information, communication technology) security and adopts security best practice.

Certainly there is the possibility for AIS, GNSS, ENC and ECDIS charts to disappear from bridge screens or be modified, but the issue today is that most adversaries want to obtain data for financial gain.

Payment systems can be easily penetrated using targeted phishing scams to raise fake invoices or even to change shipping manifests in order to transport illicit goods, drugs and weapons. The loss of sensitive data through breaches in system security is the single most important challenge that faces the maritime industry today.

This White Paper looks at the often simple ways in which criminals can obtain sensitive commercial data and provides recommendations on what shipowners and other companies operating in the maritime industry can do to mitigate the risk of a cyber attack.



Introduction

The past year has been a busy one for cyber criminals, with over 500 data breaches and more than 150 million records exposed in 2015. This includes the disclosure of 21 million U.S. Office of Personnel Management (OPM) records, the 70 million medical records at Anthem and the 37 million user details at infidelity site Ashley Madison.

January, April and July were the biggest months this year in terms of major security breaches and with the end of year looming – always a period given to an increase in data breaches – it is vitally important to remain cyber conscious and implement protective and detection measures.

The retail, technology, financial and governmental sectors head the list of business areas that were the most targeted throughout the year, though we are seeing an increase in attacks against companies operating in the transportation and critical infrastructure sectors.

Advanced Persistent Threats (APT's) are on the rise, while "ransomware" and the use of targeted phishing attacks are being used for financial blackmail and to gain access or leak sensitive, confidential information. No one is excluded from these threats and no company or individual is too small to be a target.

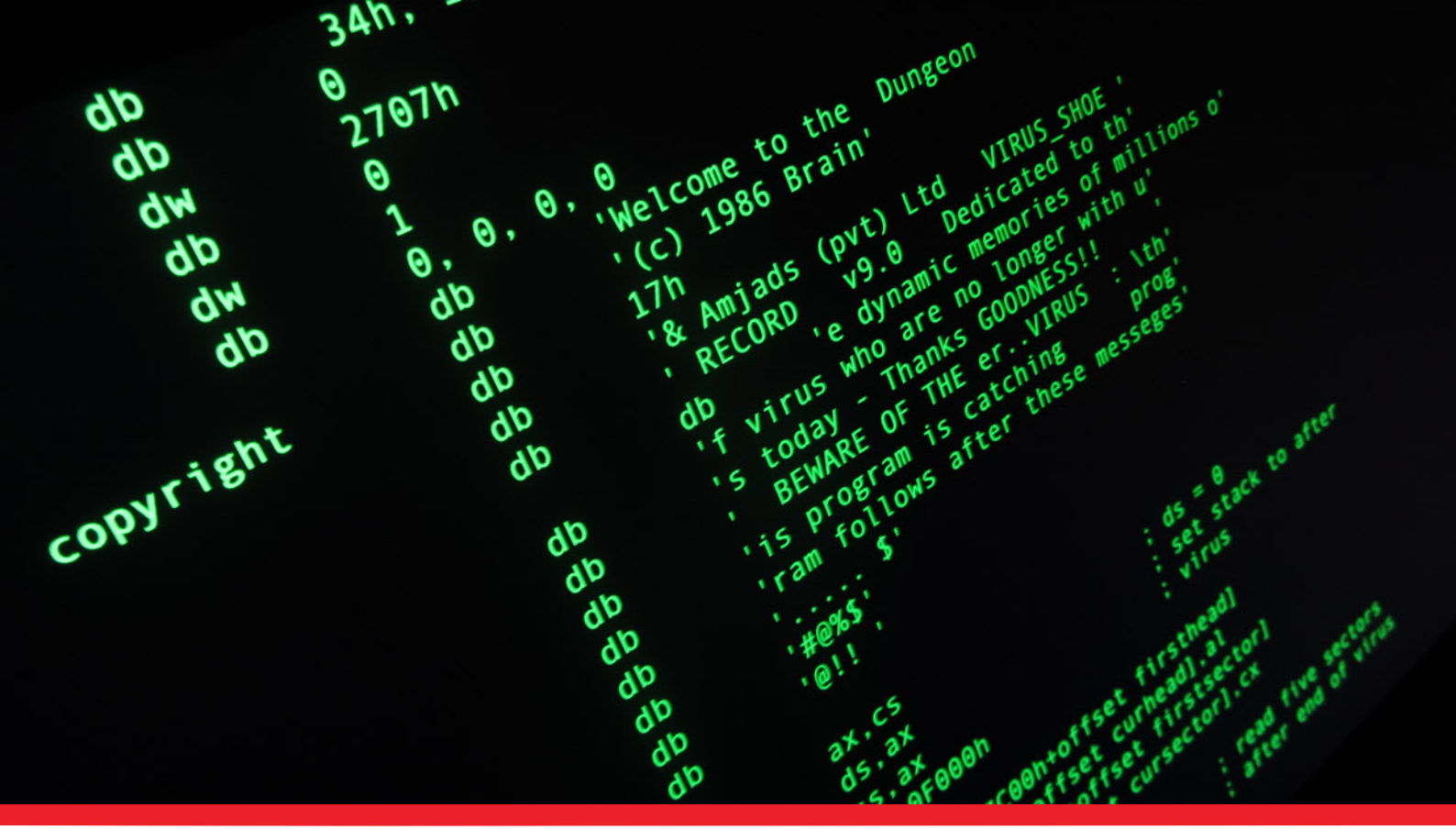
In 2015, 75% of small businesses were a target of a cyber attack and because cyber security defences are typically lacking, steps must be taken to protect data and reduce the risk of an attack.

Maritime Security & Awareness

Cyber security in the maritime industry is a major concern, due to a lack of security awareness or accountability while increasing use of new, sophisticated communications technologies raises the threat level to high. With the potential for sensitive customer data leaks via ECDIS, AIS, RFID and GPS, it is important that security procedures and processes are in place so that operators know how to identify a potential security threat or have been trained to respond when a cyber attack is in process.

The perpetrators active in the maritime industry are mostly interested in financial gain, looking to gain access, stay hidden and extract financial profit from their targets. However, accessing and extracting sensitive information or intellectual property can also help criminal or terrorist organisations whose motive is to use the industry to transport hazardous materials or weapons.

In an advanced threat, the attacker will spend a large amount of time researching a list of potential targets, gathering information about the organisation's structure, clients etc. Social media activity of the people in the target company will be monitored to extract information about the systems and forums favoured by the user and any technology vulnerabilities assessed. Once a weakness is found the next step the hacker will take is to breach the cyber security perimeter - the basic security most companies adopt - and gain access, which, for most attackers, is easily done.

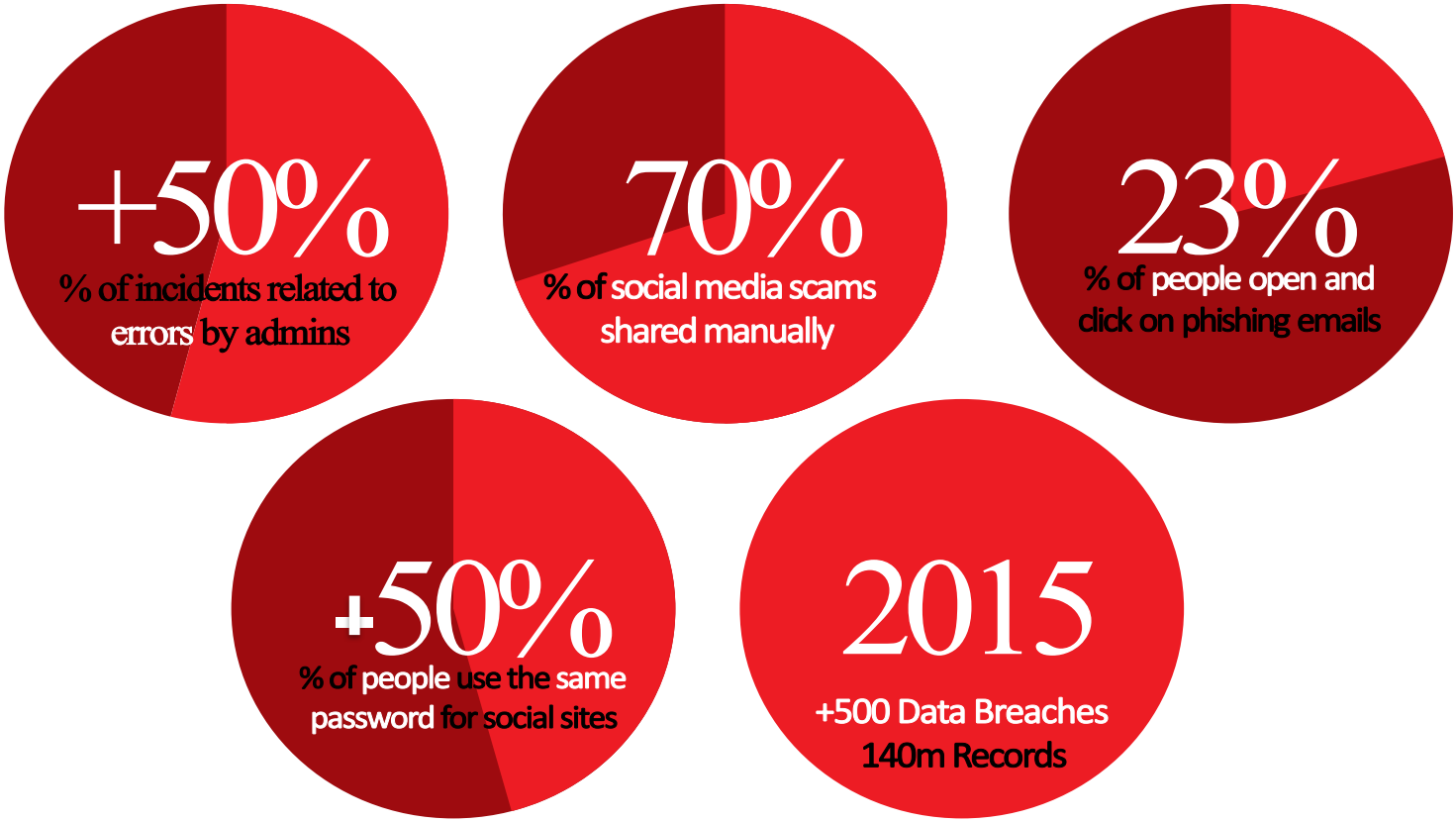


Perimeters Breached

Once inside an organisation's systems, the attacker maps the network in order to gain access to higher value assets and to elevate privilege access rights so he/she can move more freely around the company undetected.

The biggest risk is from employees using computer-based systems since security prevention mechanisms within the network itself are rearely implemented in the mistaken belief that perimeter defences are all that is required.

This, however, is where most companies need to invest more; to detect when these types of activities are occurring and reduce the breach “dwell time”. This is the period, currently averaging 205 days, before an attack is detected; a time in which the attacker has gained access, avoided detection, taken information and left without a trace.



Statistics

+50% Is the percentage of incidents caused by administrators incorrect configurations, leaving default passwords running or not changing passwords frequently, etc

70% Is the percentage of social media scams and malware being shared via social media activity

23% Is the percentage of users opening phishing emails

50% Of users use the same password on personal accounts as they do for their corporate ones

99% Of all cyber-security breaches are from known vulnerabilities

90% Of known vulnerabilities have security patches available

+25% Is the percentage of cyber attacks that can be averted with increased cyber risk awareness

Patching Systems

Another major concern is the ever growing and increasing complexity of patching systems and applications. This is typically more complicated in the maritime industry due to distribution, remote access and limited bandwidth available as well as poorly trained end-users operating these technologies. The importance of "patch management" is huge since it can mitigate more than 80% of cyber threats, leaving only those nasty zero days to deal with. Vulnerabilities are growing each year and out of the exploited vulnerabilities in 2014, 99.9% of them had a CVE (Common Vulnerabilities and Exposures) published.

Passwords & Privileged Users

Passwords and privileged accounts should be a major concern for many organizations. These can be the difference between a simple low-severity cyber breach and a high-severity cyber breach.

Companies should provide suitable training for employees on best practices for password choices, normally a very complex password is required though many employees revert to writing them down due to difficulty in remembering them or use the same password for corporate and personal social accounts. This leads to a possible external threat which companies should continuously assess.

If your company is giving employees local administrator accounts or privileged access then this seriously weakens the organisation's cyber security. This can mean the difference between a single system and user account being compromised and the entire organisation's computer systems. In all Advanced Persistent Threats the use of privileged accounts have been the difference between a simple perimeter breach and a major data loss, malicious activity or financial fraud occurring.

Organisations should quickly ensure that they continuously audit and discover privileged accounts and applications that require privileged access, remove administrator rights where they are not required and adopt two factor authentication to mitigate user accounts from easily being compromised.

Preventative Measures

ESC Global Security recommends that companies operating in the maritime industries put cyber security awareness training at the top of the agenda for users of technology and computer resources. This is one of the most effective ways of reducing a company's exposure to cyber security threats and increases both detection and incident response at the same time.

It is highly recommend that training starts at the top of the organisation, working down. It is also recommend that a company appoints a cyber/security ambassador within each department to assist in the detection and incident response for potential cyber security threats and risks. This helps expand the efficiency of any IT security team, while ensuring that there is someone in the organisation who is responsibile and accountable for implementing and maintaining cyber security measures.

It is also important that each company has an IT Security Policy and Acceptable Ase Policy to ensure that employees and users within each company understand how company resources and data should be used. This also ensures that standards are consistent, understood and adhered to. These are important steps in developing a company-wide cyber security awareness culture.

Subscriptions to security bulletins and alarms are equally important so that any new security threats are proactively evaluated and the required risk mitigation considered and rolled out where applicable.

Companies must ensure that asset management, discovery and lifecycle management of all IT assets and resources are performed. A major but typically under utilised cyber security threat mitigation is the disposal of legacy, old systems and those with security vulnerabilities. Having an end of life policy and adhering to this will help companies keep legacy systems from exposing serious security threats and risks. This will not only reduce unnecessary costs but improve the security posture.

By patching systems on a regular basis and measuring the current patch and vulnerability state will help identify where an attack might occur next. This information should prompt you to consider increasing your detection techniques in those areas or systems.

Performing continuous cyber security assessments is another key facort in mitigating risks. While these assessments are often considered as a "checkbox" means of passing or complying with regulations, they should be approached as a method to evaluate the state of cyber security. They can be used also to evaluate incident response capabilities, detect if an active breach is in progress, and to keep the company security conscious.

A very important recommendation is to be deceptive, be unpredictable. Most organisations look to automation to help assist in their cyber security defences but in many this lends itself to predictability: scans are run at the same time every week, patches take place once per month, assessments once per quarter or per year.

Companies that are predictable are very vulnerable, so should establish a mindset in which systems are updated and assessed on an adhoc basis. Randomise your activity. This will increase your capability in detecting active cyber attacks and breaches.

And finally seek expert advise from companies like ESC Global Security. Security experts can perform Risk and Vulnerability Assessments, provide Cyber Security Awareness training, undertake patch management assessments, discover and identify privileged users and accounts and mitigate those risks where possible.

If you have a breach, ESC Global Security can provide expert and professional cyber/digital forensics to help get your business back up and running, isolate the threat and perform root cause analysis, allowing your operations to continue securely.

More information about secure passwords can be found here: http://www.informationisbeautiful.net/visualizations/top-500-passwords-visualized

And for more information relating to some of world's largest data breaches, click here: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Summary

The past year has been a busy one for cyber criminals, with over 500 data breaches and more than 150 million records exposed in 2015. January, April and July were the biggest months this year in terms of major security breaches and with the end of year looming – always a period given to an increase in data breaches – it is vitally important to remain cyber conscious and implement protective measures.

ESC Global Security has made a number of recommendations so that shipping companies, in particular, can mitigate the cyber risk. These include:

- Establish a cyber training and awarness regime
- Create a cyber/security ambassador role within each department
- Make sure you have an up to date IT Security Policy and Acceptable Use Policy
- Subscribe to security bulletins and alarms
- Patch systems on a regular basis
- Perform continuous cyber security assessments
- Seek advise from experts

About 99% of all cyber-security breaches are from known vulnerabilities and about 90% of these breaches have patches [software updates] available containing the required security fixes.

While security awareness and greater computer literacy can mitigate the risk, no one has really established best practice guidelines that specifically targets maritime industry cyber threats.

We need to act in concert so that the International Maritime Organisation has the information required to implement measures that will ultimately safeguard the maritime industry from cyber-crime and protect very sensitive data.

Cyberspace was once just a way to communicate but now pretty much everything depends on it. Our critical infrastructures for energy, healthcare, banking, transportation and water are dependent on how well we protect and secure the systems and the data that controls them.