Information Security Awareness Program

SECURITY

Monthly Newsletter — January 2010

Email: Use it with care

All of us use email on daily basis and it is an essential business communication tool. However, when it comes to sending sensitive data to another person, email is not a secure mechanism. To understand this, consider Tom is sending an email to Jerry. During this process, data goes through multiple servers as explained below and shown in the diagram:

1. When Tom clicks the "Send" button, the email is delivered to his company's email server where it is stored.
2. The email is may go through multiple email servers on the Internet where it can be copied and views by owners of those servers.
3. Eventually the email reaches Jerry's company email server where it is stored for delivery.
4. Jerry reads email after getting from his email server.

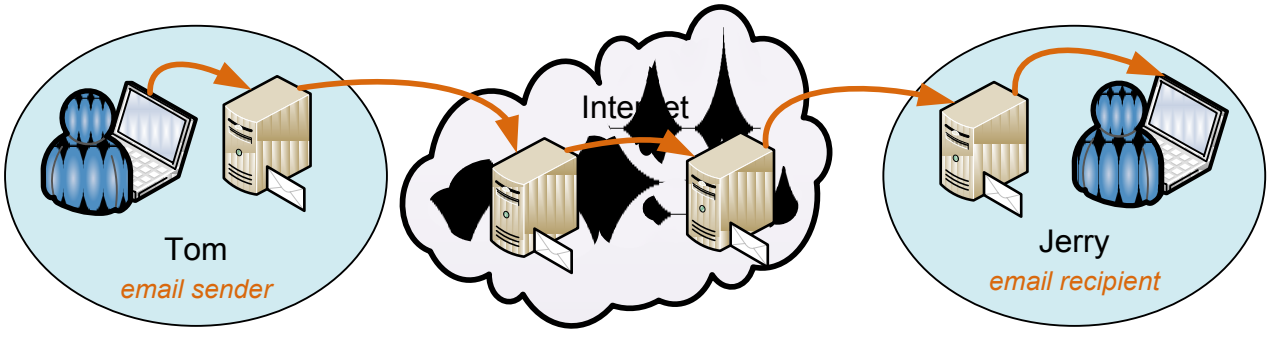
As you can see, in this process the data is stored on multiple servers, some of which may be owned by third parties on the Internet. At all of these points, the email can be viewed by unauthorized persons. So regular email can put confidential data as risk.

What is Confidential Sensitive Data?

Following are some examples of confidential and sensitive data and should never be sent via email:

- Social security numbers
- Credit card information
- Names with date of birth or addresses
- Trade secrets
- Payroll information and bank account numbers
- Company financial reports

So what is the right method of sending sensitive data to others? Each company has different mechanisms for secure data transfer. These include secure file transfer using SFTP or SSL, encrypted email, secure web sites and so on. When you have a need for sensitive data transfer, it is best to contact your information security or compliance person.



FREE CREDIT REPORTS

Most of the people may not know that you can really get a copy of your credit reports for free every year. The federal trade commission (FTC) authorized http://www.annualcreditreport.com as the only source for getting free credit report from three major credit reporting agencies (Experian, Equifax, TransUnion). The link is advertised on FTC web site http://www.ftc.gov/freereports. You can request your free credit report from all three agencies online, by phone, or via email. Once you have the report and you need to dispute anything in your report, you can contact individual agencies. You can also put "fraud alert" on your file if you believe your identity has been stolen. You can call any one of the following three agencies to put fraud alert.

Equifax: 1-877-576-5734; www.alerts.equifax.com
Experian: 1-888-397-3742; www.experian.com/fraud
TransUnion: 1-800-680-7289; www.transunion.com

Protect Your Identity and Review your Credit Report at least once a year

DATA BREACH REPORTS

Companies like Verizon and 7safe publish research about data breaches regularly. According to Verizon report published in 2009, **285 million records were stolen** in 2008. The interesting thing is that many of the breaches are caused by simple things like leaving default passwords unchanged and configuration errors that can be easily avoided. Verizon security blog is at URL http://securityblog.verizonbusiness.com/

SOCIAL MEDIA WEB SITES

Do You *Really* Know

Who is on the other side?

CLOUD SECURITY

Make Informed Decisions for Cloud Migration

Cloud Security Alliance (http://www.cloudsecurityalliance.org/) and European Network and Information Security Agency (http://www.enisa.europa.eu/) recently published guidelines and risk assessment for cloud computing. These are detailed reports covering a multitude of issues related to cloud computing. These documents are also very good for understanding different aspects of cloud computing, like:

- Different types of clouds
- Issues related to legal and compliance aspects of cloud computing
- Encryption and data security
- Managing identities
- Trust in cloud computing
- Issues related to reliable audit
- Insider threat and governance

According to analysis done by IDC, in 2013, worldwide market for cloud computing will reach

$44.2 billion

Cloud computing security and privacy issues will become more visible as the market grows. These documents are very important for professionals working in information security and privacy sectors to understand current and future issues related to cloud computing. Making informed decisions is key to successful transition to cloud computing.

The reports are available at the following links:

- http://www.cloudsecurityalliance.org/csaguide.pdf
- http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Important Compliance Links

There are links for important web sites from compliance perspective:

1. **Payment Card Industry (PCI)** Security Standard is a standard for companies that handle credit card data
   https://www.pcisecuritystandards.org/
2. **Sarbanes-Oxley (SOX) Act** is for publically traded organizations
   http://www.sec.gov/about/laws.shtml
3. **Health Insurance Portability and Accountability Act (HIPAA)** is for companies that deal with medical information.
   http://www.hhs.gov/ocr/privacy/