Cyber Security for Financial Institutions

By : Khawar Nehal
http://atrc.net.pk
9 January 2019

Why Cyber Security

It is a part of risk management.

Profitability is related to risk management.

If you take unnecessary risks, like those which can be mitigated but are not prepared for, then compared to the competition, the institution shall perform worse and shall in the long term be at the risk of being merged or taken over by other better performing institutions.

Why Cyber Security

There are two major issues as to why financial institutions are in the state they are in today as regards to computer security.

They have not decided to take responsibility for all of the systems they manage down to level of detail as compared to other organizations that use computers like ISPs, Telcos and ecommerce providers.

Why Cyber Security

The root cause for this difference is due to the attitude which financial institutions take towards the use of computers.

They believe that computers are a part of their business and sort of secondary to customer support.

The other organizations like ecommerce, ISPs and telcos KNOW that managing the computers is their prime business. This is the reason they have a customer.

Outsourced

This difference in attitude results in the difference in how it is managed.

Most financial institutions use auditing firms for compliance to regulations.

So when the regulator comes up with something new, they call the auditing firms to “deal” with it.

Outsourced

The opposite is true for the organizations which are proactive in managing computers.

The ISPs, telcos and ecommerce never think that any third party having no ownership of the company shall be able to go into detail required to analyze the design, system, software and even the hardware required to be called responsible for the whole system.

So they hire all the experts in house to deal with it.

Large task in pieces

Since the serious organizations know they are to take responsibility for each line of code and each circuit design in the hardware, they are ready to share their results in order to achieve the analysis detail necessary to complete the task.

An example is Google. They hired zero day experts and that department was able to find bugs in hardware and software which were not found by the vendors.

Vendor dependency

The financial institutions on the other hand have the attitude that they need to depend on the vendors to do everything.

This boils down to the resulting vendor terms.

Yes these are real and you do press the I agree and do agree to these terms on a daily basis because you do not care about what you are agreeing to.
That is why we have this issue in the first place.

Vendor term samples

Do not criticize this product publicly.

Using this product means you will be monitored.

Do not reverse-engineer this product.

Do not use this product with other vendor's products.

By signing this contract, you also agree to every change in future versions of it.

Vendor term samples

Oh yes, and EULAs are subject to change **without** notice.

We are not responsible if this product messes up your computer.

No warranties

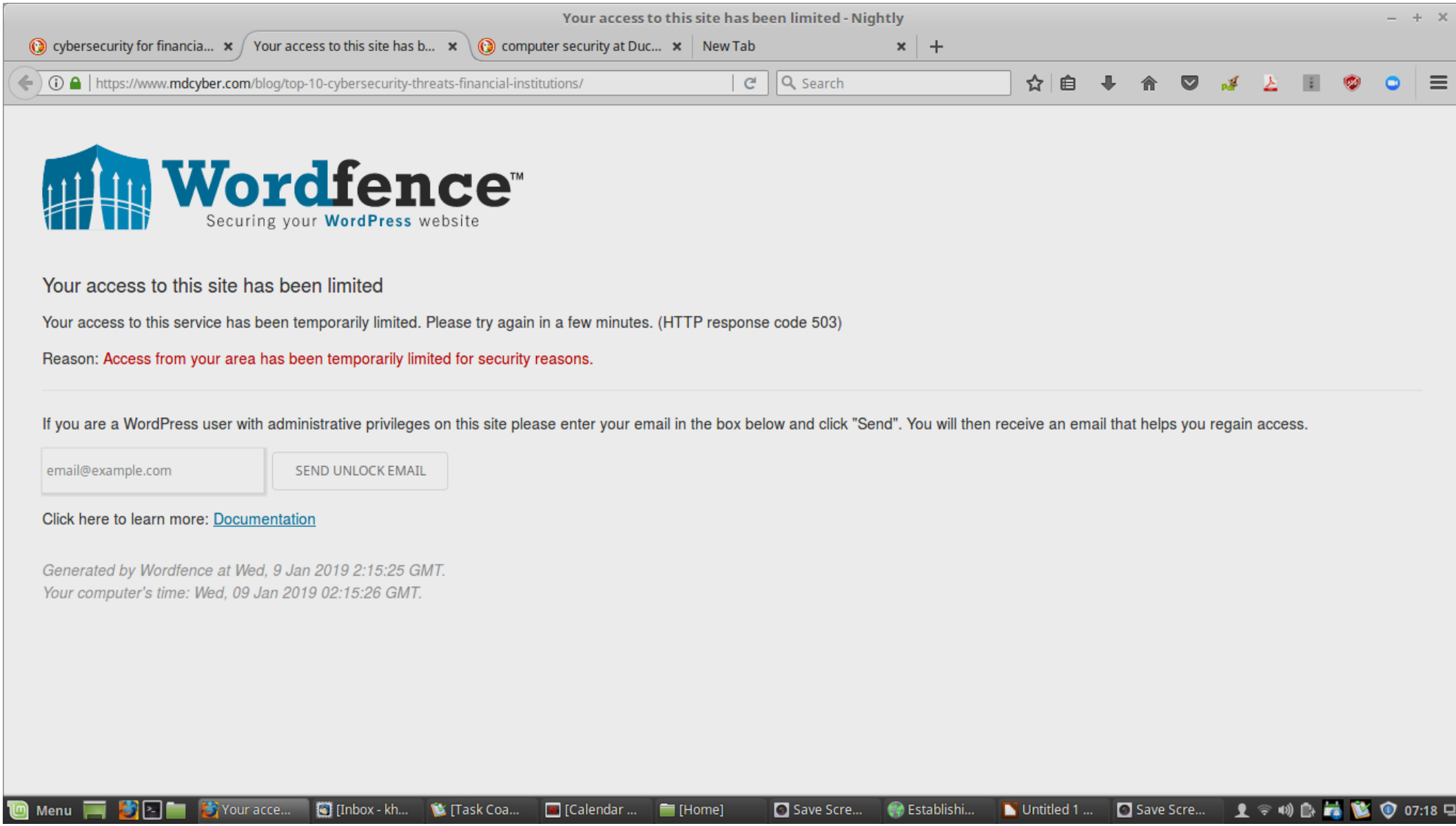
No liability for any damages even if the product fails of its **essential purpose.**

Vendor term situation

How did the vendors get so far in their impossible and one way terms ?

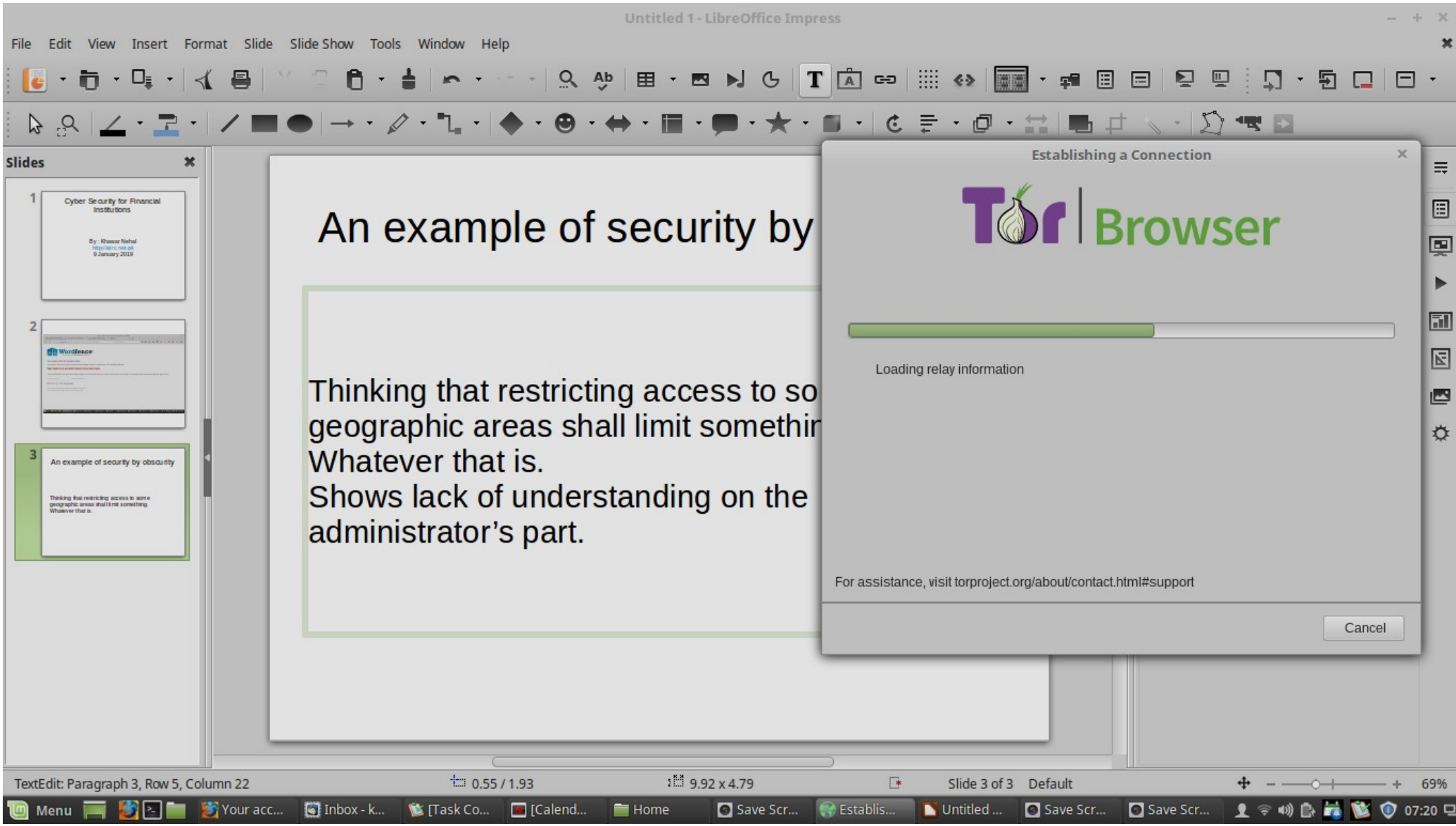
Blame the buyer.

Placing too much trust and **NOT** auditing the vendor terms is the **ONLY** reason why things are in such a dire straits for financial institutions.


Your access to this site has been limited - Nightly
cybersecurity for financia...
Your access to this site has b...
computer security at Duc...
New Tab
https://www.mdcyber.com/blog/top-10-cybersecurity-threats-financial-institutions/
Search
Wordfence™
Securing your WordPress website
Your access to this site has been limited
Your access to this service has been temporarily limited. Please try again in a few minutes. (HTTP response code 503)
Reason: Access from your area has been temporarily limited for security reasons.
If you are a WordPress user with administrative privileges on this site please enter your email in the box below and click "Send". You will then receive an email that helps you regain access.
email@example.com
SEND UNLOCK EMAIL
Click here to learn more: Documentation
Generated by Wordfence at Wed, 9 Jan 2019 2:15:25 GMT.
Your computer's time: Wed, 09 Jan 2019 02:15:26 GMT.
Menu
Your acce...
[Inbox - kh...
[Task Coa...
[Calendar ...
[Home]
Save Scre...
Establishi...
Untitled 1 ...
Save Scre...
07:18

An example of security by obscurity

Thinking that restricting access to some geographic areas shall limit something.
Whatever that is.
Shows lack of understanding on the administrator’s part.



+92 343 270 2932 khawar@atrc.net.pk http://atrc.net.pk

Activated tor to go around lameness

Third party providers

Awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks associated with them.

To identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

7 decades of “computerization”

Financial institutions found out that they are increasingly dependent on information technology and telecommunications to deliver services to consumers and business every day since the 1950s when computerization started. Knowing that disruption, degradation, or unauthorized alteration of information and systems that support these services can affect operations, institutions, and their core processes, and undermine confidence in the global financial services sector is a known for the past more than 70 years. So it is not news. Talking about it as such show that the person has no clue as to the history of the subject.

Gaps

Somehow after these decades of sleeping and being continuously under threat of attacks, the financial institutions seem to have realized the reality that by having a licensee to do transactions from the government and having the government police on their side shall not stop them from being successfully attacked and robbed. The regulators who have done a great job of monitoring the frauds via looking at illegal transactions also realized that anonymous tampering via global perpetrators using links across gateways placed in international waters shall provide no teeth to them to prosecute any perpetrator they cannot trace at all in any legal way. And they cannot prosecute any perpetrator they do not have the the means to trace.

Gaps

Somehow after these decades of sleeping and being continuously under threat of attacks, the financial institutions seem to have realized the reality that by having a licensee to do transactions from the government and having the government police on their side shall not stop them from being successfully attacked and robbed. The regulators who have done a great job of monitoring the frauds via looking at illegal transactions also realized that anonymous tampering via global perpetrators using links across gateways placed in international waters shall provide no teeth to them to prosecute any perpetrator they cannot trace at all in any legal way. And they cannot prosecute any perpetrator they do not have the the means to trace.

Cyber insurance

The idea of coming up with a fund for cyber insurance as a risk management strategy is basically a way to spread the risk among financial institutions and is a way to declare that they are all in the same boat.
If most agree then the regulators shall force all of them to take this insurance.

The major risk is that the risky participants shall become more relaxed that they have somehow shoved the issue under the carpet for a few more days and bought some cover from risks which they should have mitigated in the first place and still need to deal with.

This idea has been floated in 2018. Lets see how long it takes the regulators to implement it.

Risk Trends

- **Existing vulnerabilities continue to be exploited**

  Easily exploitable vulnerabilities persist

- **New platforms create new cyber attack opportunities**

  New ways to exploit financial institutions and their customers

- **Lines between cyber actors are blurring**

  Commercialization of tools, resources, and infrastructure

Risk Trends

- **Tactics evolve in response to online behavior**

  Social networks enable more effective and targeted attacks

- **Trends in malware are evolving**

  Destructive malware and cryptographic ransomware

Services more easily procurable

Cracking services and malware development services are likely to be more easily available as the public becomes aware of the lack of security capability of the financial institutions.

The most dangerous threats are present when a cracking expert, malware developer/supplier, penetration tester and security penetration tester work in tandem to prepare an attack. And if they have an guru level hacker/developer on their team, they could penetrate almost any system.

Risk Trends

Potential Impacts

- Financial
- Operational
- Legal
- Reputational

Owners need to take ownership

It is now time that the owners have realized that their lack of capability to reduce costs, increase performance and maintain security has provided a huge opportunity for the telecom, post office, ISP and ecommerce sector to come together and provide financial services. All they need is a financial license to meet local and global regulations.

Owner need to take ownership

Telecom provides the secure transaction and communications infrastruture
The post office provides the branches for customer services and home delivery services.
The ISPs take the telecom to the home.
Ecommerce brings in the suppliers and shops.
In Pakistan, two telecom companies have bought banks in this trend and shall be integrating to get the competition going.

Examples of competition

Recently my colleague sent me this news item.
I shall use it to explain the status quo and explain what the future looks like to me.
Feel free to improve on the predictions and provide feedback.