Case Study

Online banners are often used to enhance consumer confidence in making purchases online, but what implications are these if these online claims turns out to be false?

There was a difference of opinion about the term “online banners”, thus we give two answers with the third paragraph being part of both.

An online banner from a company can and should be considered as a formal statement from the company with regards to the banner text, and can thus be considered a contract. Thus if you claim security but fail to provide said security it should be on the same level as any other contract breach. An analogy would be a salesperson in a retail store claiming that product A can do x, but if it turns out product A can't do x then it's within reason for the consumer to claim a breach of "contract" with the retailer as they've sold a product based on a feature that doesn't exist.

The use of an online banner, is commonly used to ensure the sure that the site they are connected to is in a way legit.. tho one might not be so sure of it when looking at it. But the sense of knowing that the site is legit is thou somewhat hard for those who don't browse the net regularly. For one that does a lot of online shopping knows what to look for when they are presented with a site that might be fake. Some criminals just set up these webshops with incredible insane prices on high quality brands like iphone or rolex, just to scam people for their personal details as name, number and credit card info is probably the most rewarding of them all. Not much one can do with a name but one and do lots with the credit card info. One can quickly distinguish a real shop from a fake depending on how they looks. In example if there are two shops. Shop number 1 have a site that is really professional looking, and has everything from legal terms to good looking design.. Shop number 2 has a semi-pro looking site but is missing crucial information.

The short term implications may be a general lack of trust of online sites and possibly a decrease in sales. The long term implications could be changes to the laws governing online sales and the security measures involved in online transactions and other security information.

How can a company ensure that it takes "reasonable or appropriate measure to prevent personal consumer information from being accessed for illegitimate purposes?

For a smaller company using a well known online retailing package, while keeping the backend systems up to date is an appropriate measure on the technical side.

A medium to larger company will want to hire a red team to test their implementation, and have continuous monitoring of their infrastructure and IDS. The company may hire white hat hackers, to check if the customer information is secure and not accessible for intruders.
In any matter the use of hashing and encryption for sensitive information,passwords, credit cards and similar, is a minimum.The ecommerce site should also use Secure Socket Layer (SSL), such as HTTPS. Such that sensitive information, such as username/passwords, credit cards and similar, can't get accessed in transit. On an added note Firefox and Chrome users will get a warning when they try to type sensitive information into non-secure fields. Which will discourage users.

From a formal standpoint any customer facing interactions will need a set of procedures used to verify an existing customer, and a policy on which details they can give out and change over phone/email without further verification.
There should also be formal guidelines for customer interaction.

A company or a site can never be 100% safe, but the best it can to is to monitor the online security situation and implement security measures to new threats as soon as they are available.

What implications does this case hold for persons involved in information security?

The implications is that when a company gives a statement, they must be able to back said statement up. If not, unknown individuals might get a hold of customer information.

The case also serves as a reminder to security staff that the company they work for may not be giving them the tools they should have in order to do their job.

Case Study

What procedures could help prevent a similar breach of security at your organization?

Upon setting up the contract with company X, one should establish a trusted channel to exchange for example credentials and similar information. This could be a specific email or phone number where all such interactions should take place.
In the case of using phone the employee handling the call should hang up and call back on the trusted channel, as a step in verifying the source is trustworthy.
In the case of email, one should in 2017 aim for setting up Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) etc. to verify the source, and making spoofing harder/impossible.

The company could host security courses that teaches the users to be careful and critical to unknown emails and phone calls, and also show why these policies are in place. The users should use passwords that are hard to find out, as per the NIST guidelines.

To quote Mitnick himself “Just say no” if it violates policy.

Phishing(the practice of luring unsuspected Internet users to fake web sites by using authentic looking email) Is usually associated with identity theft, but could this tactic also be used to gain information needed to circumvent security controls?

Yes, you can phish for valid credentials that can later be used for authenticating through for instance Virtual Private Network (VPN) or similar. For example University of Agder (UiA) has had multiple emails where a third party pretends to be from the IT department and you have to adjust your email quota by supplying the needed amount of space, and your username/password.

A hacker could also impersonate the service desk phone and call up users telling them to let him connect to their computer. Then he could access the server or other confidential information that is stored on the user's’ computer.