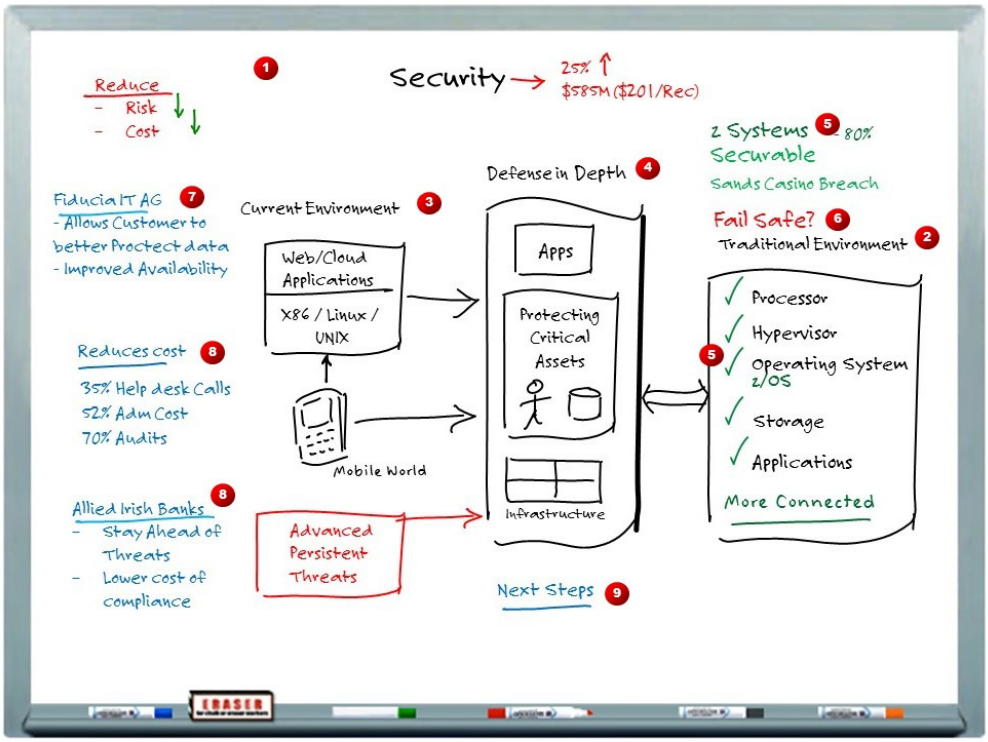
Security on z Systems™

Solution Whiteboard Storyboard

Version 2015-07-29 @ 5;53PM

Original template used by permission of Corporate Visions, Inc...

OVERVIEW



Purpose

This whiteboard is intended to help **sellers** better understand and be able to discuss the **importance of** having the right security structure on z Systems. The whiteboard should enable a seller to have an interactive (Discovery & Qualification) discussion that not only helps to uncover the key client challenges and issues with respect to security on z Systems, but also enables the seller to describe at a high level that security on z Systems just does not happen by itself. z Systems is the safest box, but it has to be monitored and continuously updated to avoid threats.

The whiteboard is also intended to help get **hardware and software sellers** involved to better understand why z Systems is the most secure system in the industry, but that it does not "just happen". Instead, monitoring and continuous updating are needed. If this is ignored, z Systems could be breached.

This whiteboard can be used to do a cross-sell of our security products on processors other than z Systems. It can also be used if the customer is considering moving applications off the z Systems platform.

Target Audience

The customer target audience for this discussion is the IT managers with overall responsibility for z Systems. The CISO can be included in this meeting or can be a "next step" in the form of a briefing.

Goal

The goal of the whiteboard is to get agreement for one of the "next steps" described in the Appendix.

Original template used by permission of Corporate Visions, Inc..

Pre-Discussion Preparation

You should always check the Whiteboard Media Library **(http://w3.tap.ibm.com/medialibrary/media_set_manage?id=38381)** in preparing for this whiteboard to ensure you have relevant and appropriate references and customer stories and that you are prepared to cover the areas that may be important to the audience.

Whiteboard Discussion Steps

Discussion Steps in this whiteboard are:

1. Setting the Stage
2. Traditional Environment
3. Current Environment
4. Defense in Depth
5. z Systems
6. Fail Safe
7. Reduced Risk Customer Example
8. Reduced Cost Customer Example
9. Next Steps

Legend for Colors

Color in this whiteboard is used to indicate the following:

Black - FACTS or subjects that frame the discussion

Blue - Topics that we want to emphasize, typically action-oriented, i.e., someone is going to do something (outlining what we will discuss, for example) or has done something (customer story – **which you can add to this whiteboard**)

Red - Challenges or items that most people do not take into account in developing TCO

Green - Action or activity that either overcomes an issue or provides a positive outcome

The items you should draw are shown in **[BOLD] in the color you should use**

NOTES TO PRESENTER:

Do your homework before the meeting. Understand as much as possible about the audience – What is their current security environment? Have they had any breaches on x86? Linux®? UNIX®? z Systems? What was the cost of these breaches?

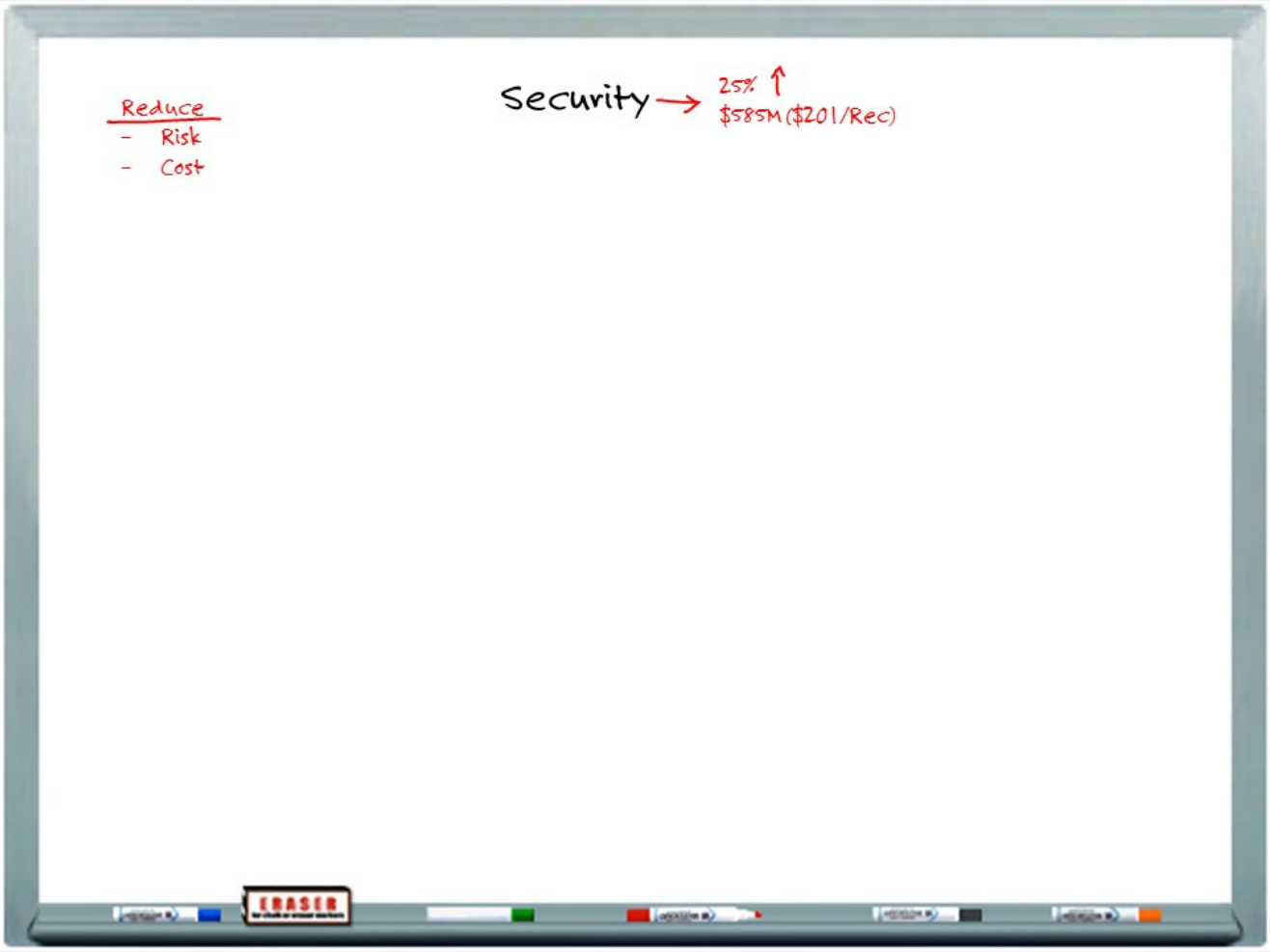
You should be prepared with customer examples that will be relevant to the audience in terms of industry, region, size of organization, and so on.

Many of these opportunities may involve or may need to involve other IBM teams. Make sure that you are working with your counterparts on other teams to help you to maximize the opportunity.

You will notice a list of questions with most steps of this whiteboard. They are designed to help you develop a conversation between you and the client.

Original template used by permission of Corporate Visions, Inc..

1. SETTING THE STAGE



Thank you for taking the time to meet with me today. Recently, we had a discussion about security. **<WRITE "Security" >** As we discussed, **<WRITE "25%" and DRAW up arrow >** recently there was a report concerning the increase in breaches during the past year. And on an average, these breaches cost $585M, or an average of $201 per record. **<WRITE $585M ($201/record)>** You stated that you had been concerned particularly after some high-profile accounts were breached. And, you were interested in reducing your risk exposure and the cost of securing your environment. **<Write: "Reduce" and DRAW line under it, WRITE "– Risk" on the next line followed by "– Cost" on the following line>** Are there any other concerns?

NOTE TO PRESENTER: If the client asked where we got these numbers, they came from the IBM

Original template used by permission of Corporate Visions, Inc..

X-Force Threat Intelligence Quarter Intelligence Quarterly Report, 1Q2015.
http://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03073usen/WGL03073USEN.PDF

QUESTIONS TO ASK:

- To what sort of risks do you think your organization might be exposed?
- Do you feel like you can measure your risk exposure?
- Do you have a sense of what a major breach could cost your organization?
- Do you have a sense of what you are spending now to prevent breaches**?**

POTENTIAL OBJECTIONS & RESPONSES:

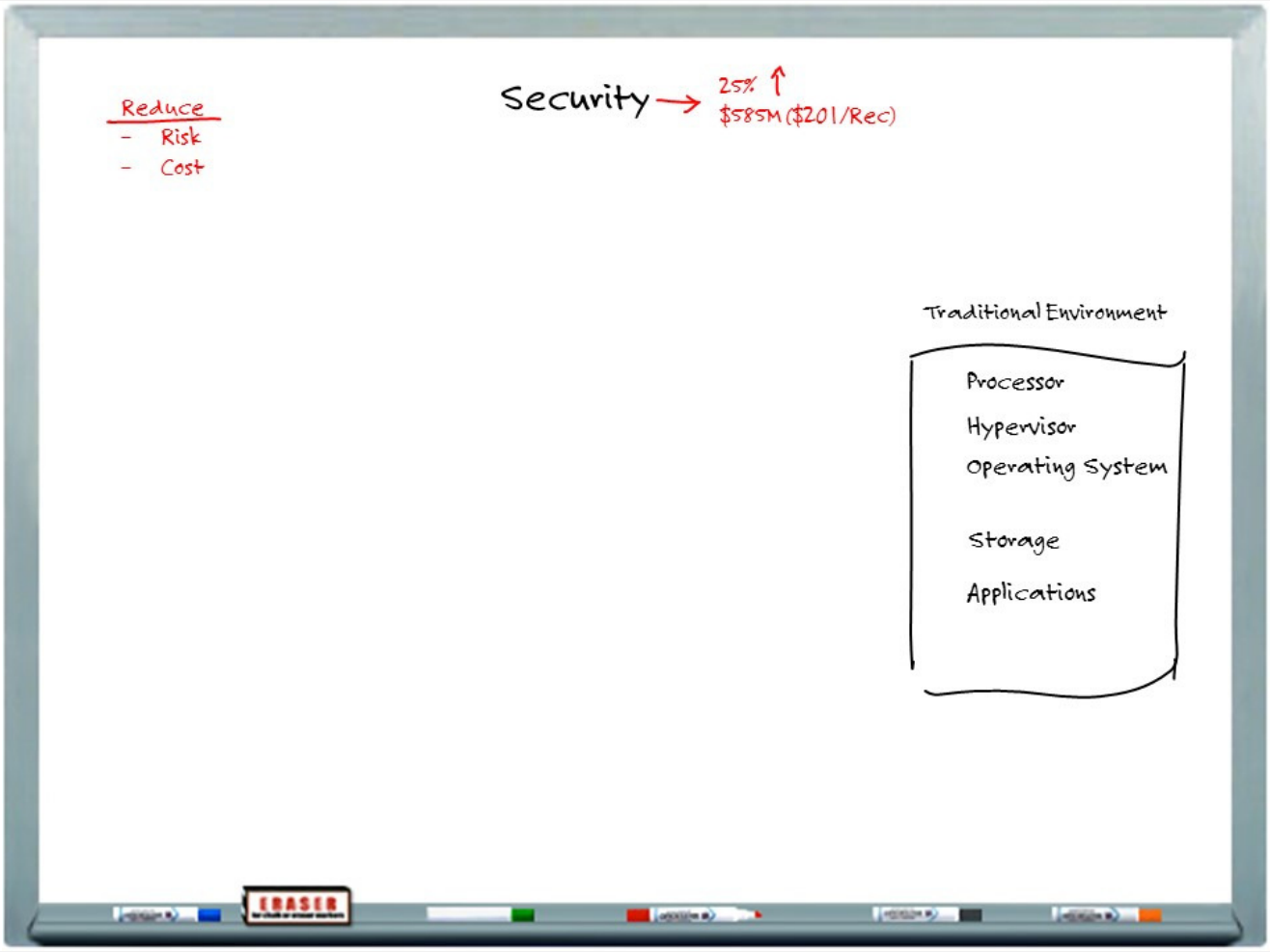
OBJECTIONS:

We were audited recently and no major risks were identified.

RESPONSE:

IBM has a security department called X-Force®. This group of professionals continually identifies new risks. Do you feel comfortable that you have the layers of defense in place to protect your organization against unforeseen risks?

2. TRADITIONAL ENVIRONMENTS



When talking about security, it's important to look at your total environment. Let's begin this discussion with your traditional environment. **<Write "Traditional Environment" and Draw a curvy box below it. Leave plenty of room to have 5 lines of data within the box>.** Security begins with the hardware. All parts of the hardware play a part in security.

<Write "Processor" in the box> everything always begins with the processor. Most systems today have multiple processors. All operations have to go through the processor, and if you ask the processor to do more (that is, encryption or compression), then it can affect performance. For this reason, many clients may minimize the usage of encryption and compression.

<Write "Hypervisor"> Some systems combine Hypervisor with Operating Systems Others separate into 2 entries. **<Write "Operating System">** The basic function of the Hypervisor is to partition the system into multiple parts so that multiple operating systems can run in a single box. This includes the amount of storage and the processors which are available to that operating system. The function of the operating system is to dispatch work to the processors and to define the environment in which the application will to be running as well as

Original template used by permission of Corporate Visions, Inc..

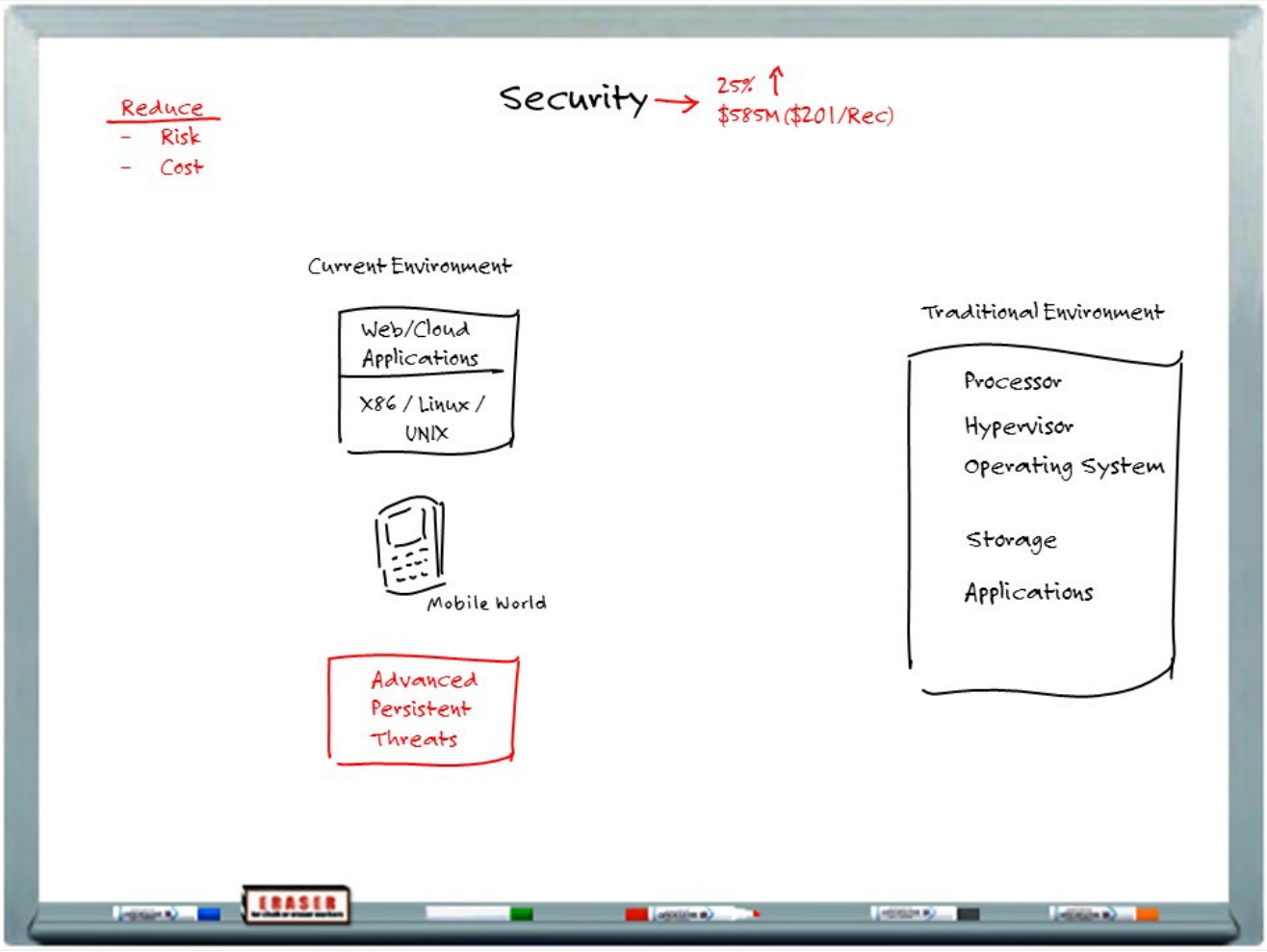
defining the rules by which the application must abide. As you can tell these two items must work closely together.

<Write "Storage"> We are talking about multi-levels of storage, from memory to disk to tape storage. Some of these may contain encrypted data. But all storage levels have security implications.

Finally, **<Write "Applications">** we come to applications and how they are written. There are methods of designing and coding applications that make them less vulnerable to attacks.

Original template used by permission of Corporate Visions, Inc..

3. CURRENT ENVIRONMENT



But this is not the environment we all live in today. So let's look at the environment we have today. **<Write "Current Environment" and DRAW a curvy box beneath, leave room for a row of information to the left >.** We live in an environment where using web browsers and cloud applications is an integral way of doing business today. **<"Write Web/Cloud Applications" in top half of box "Divide box with Line>** These applications tend to run under Windows, Linux and UNIX. **<Write "Windows /Linux/UNIX" in the bottom of the box>**.

<Draw a MOBILE DEVICE and Write "Mobile World"> We also live in a mobile world today, where your clients want their data instantaneously and your employees want to do their work anytime from anywhere. Anytime you add another environment, you complicate your security environment. For instance, mobile could be accessed from unsecured networks that introduce new avenues of attack.

And, finally, we have what is called Advanced Persistent Threats. **<Draw a curvy box, Write "Advanced Persistent Threats" in the box>** These are a set of stealthy and continuous computer hacking processes, often orchestrated by a human or humans targeting a specific entity. This is not

Original template used by permission of Corporate Visions, Inc..

an IBM definition, but rather, an industry definition. In fact, recent statistics indicated that a record 8000 new vulnerabilities were discovered last year alone.

QUESTIONS TO ASK:

- What does your overall IT environment look like today? Where is your mission-critical data stored?
- What tools and technologies are you and other departments using to secure your environment?
- What new technologies are you deploying? Are you adopting private or public cloud?
- Is your organization exploiting public clouds in any way for email or file storage or decision support systems?
- Are you experiencing any new vulnerabilities?

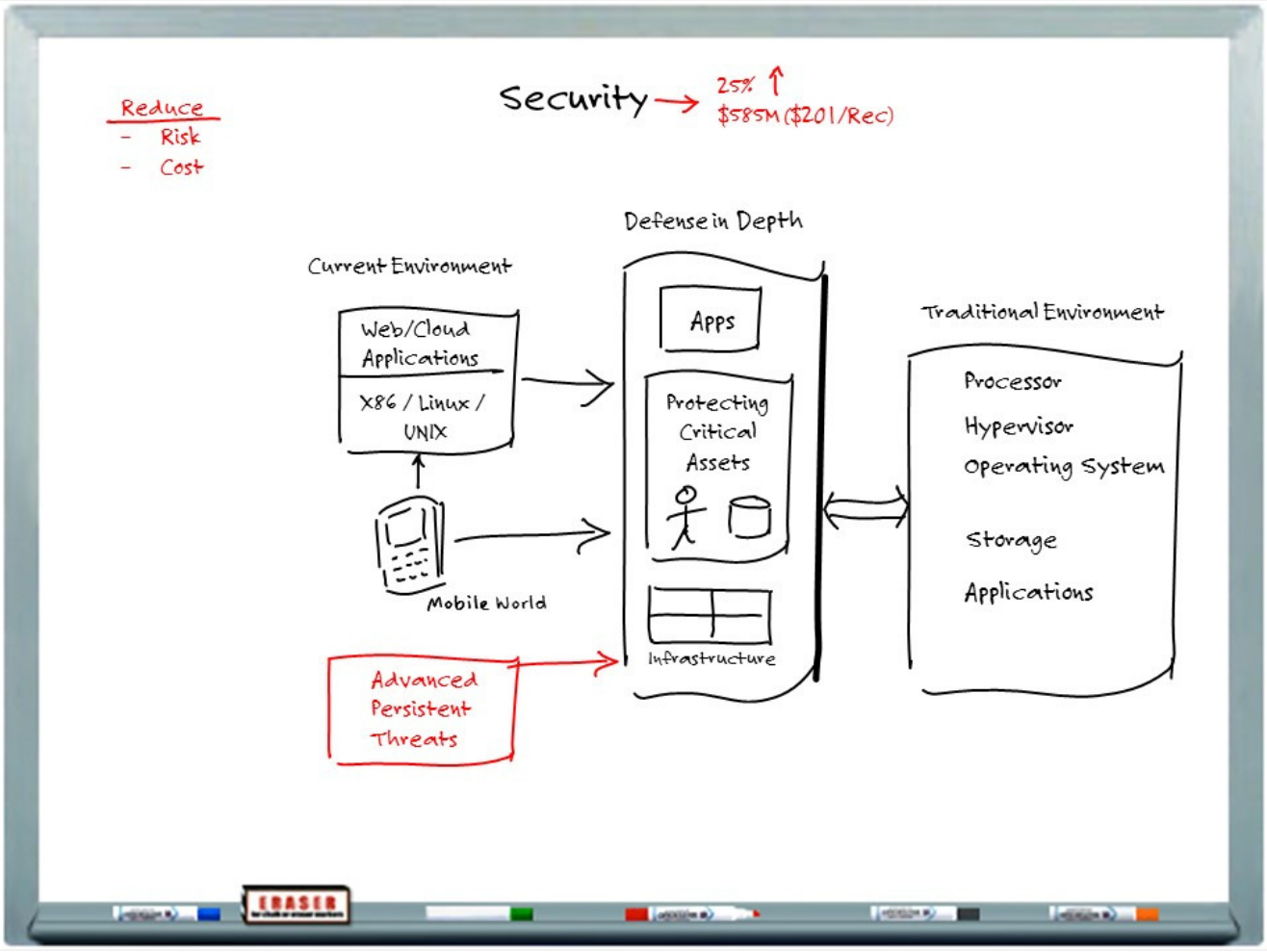
POTENTIAL OBJECTIONS & RESPONSES:

OBJECTION: Why should we be concerned about security with cloud?

RESPONSE: When you are dealing with the cloud, you tend to be using the Internet more than you would if you were tightly controlling all the access points. Also, your control is less and exposures are greater if you are talking about a public cloud.

Original template used by permission of Corporate Visions, Inc..

4. DEFENSE IN DEPTH



<Write "Defense in Depth" and Draw a long curvy box below it> Since perimeter defense is no longer good enough, the industry has come up with a new strategy called "Defense in Depth." This is a multi-layer approach to security. Products are available that will monitor some of these in real time; others will require you to run scan programs looking for issues; and yet others will require you to run analytics against logs looking for a problem that is brewing.

Defense in Depth covers 3 major categories. The first is applications. **<Draw a box in the "Defense in Depth" box and Write "Apps" in it>** Threats to applications come in many forms. The way an application is written can make it a larger target for exploitations via invalidated inputs, poor coordination between applications, mobile and web applications that are hacked with malware, and so on. Protecting applications involves several disciplines:

- analyzing applications for potential vulnerabilities
- hardening applications to protect them against hacking, particularly mobile applications, and
- monitoring network traffic flows to detect and protect against application exploits

Original template used by permission of Corporate Visions, Inc..

<Draw a long box within the Defense in Depth box and Write "Protecting Critical Assets"> Some of the largest threats come from within our clients' organizations. **<Draw a stick man>** First is your people. You are likely to have key people with unnecessary access to a large amount of your mission-critical assets. Your access programs may not be preventing your staff from being over-authorized. Throughout your organization, you are likely to have authorizations in place that are no longer needed.

<Draw a Disk> Data is another area of concern. First, we find data that should be encrypted, but it is not. Many organizations minimize the amount of encryption due to their perception of performance impact. Second, your employees are likely to be over-authorized for data. We find many customers fail to have effective monitoring systems in place to ensure mission-critical data is accessed properly.

<Draw a smaller horizontal box with hash marks in the bottom of the Defense in Depth box - Write "Infrastructure" below the box> Infrastructure is how your system is connected and protected from a networking standpoint. Defense in Depth should continuously monitor how the system is configured. Your environment is comprised of many levels of middleware. Any of these levels (communications, transaction managers, database managers, and so on) can be points of vulnerability if not configured properly.

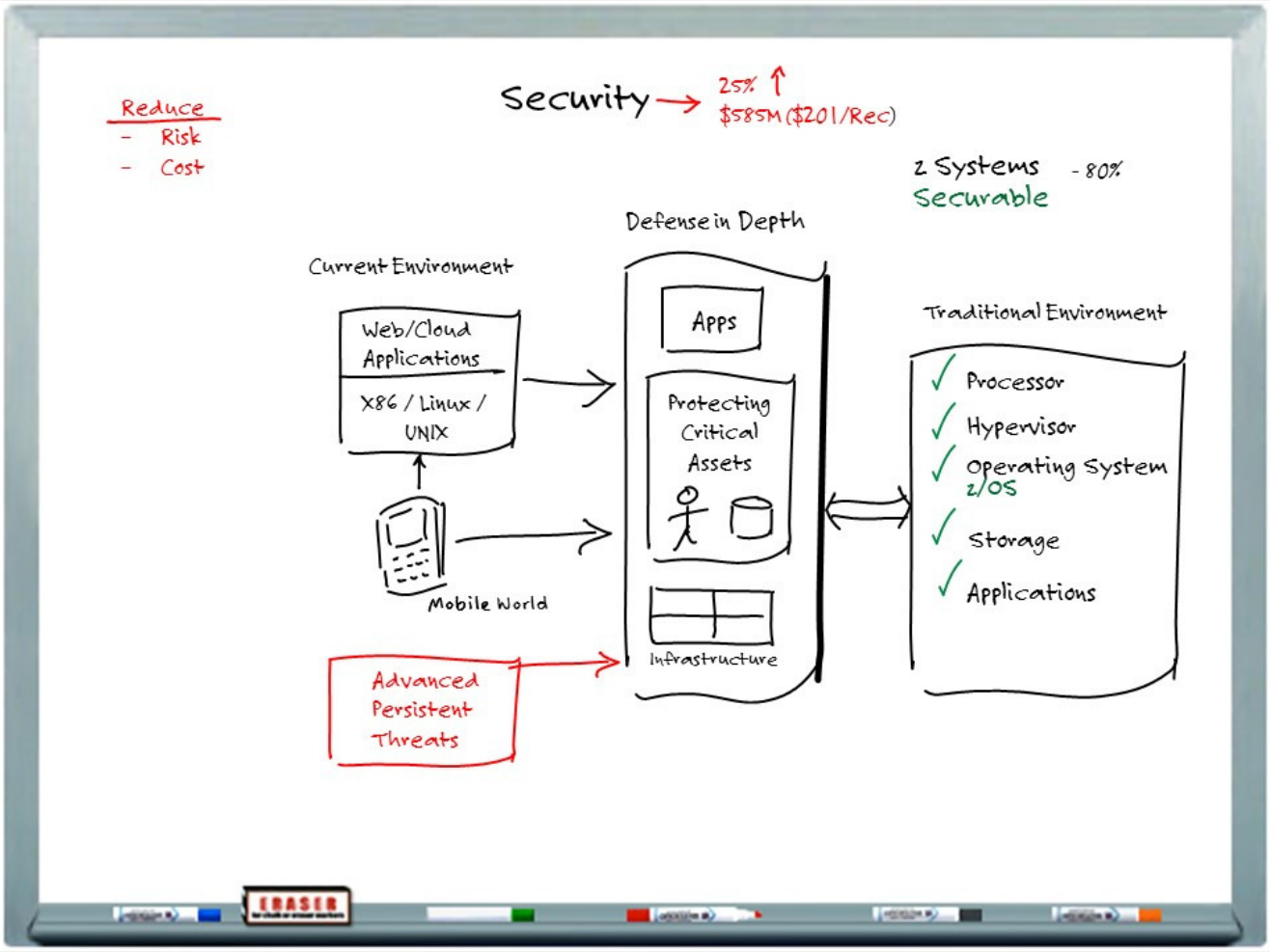
<Draw a vertical single arrow between Mobile device and the cloud box> Most customers today have the mobile devices come into a distributed box. But they can come into your z Systems box. But, these mobile devices should be going through your Defense in Depth process. **<Draw a horizontal single arrow between the Mobile Device and Defense in Depth box>** In fact all of your input into your z Systems should go through your Defense in Depth Process, regardless where the input is coming from. **<Draw a single horizontal arrow between Cloud Box and Defense in Depth> <Draw single horizontal arrow between Advanced Persistent Threats box and Defense in Depth> <Draw a double arrow between Defense in Depth and z Systems Box>.**

QUESTIONS TO ASK:

- How can you be sure that your administrators and other staff are not misusing their access?
- How can you be sure that your staff has the right level of access, no more and no less?
- Do you have effective systems in place to monitor the access of your key staff?
- Do you have effective separation of duties throughout your enterprise?
- Do you know where your mission-critical data is hosted?
- Do you have encryption systems in place for all of your critical data?
- Do you have effective monitoring systems in place for all of your critical data?
- Have you considered moving to Defense in Depth?
- What tools and technologies is your organization and other departments using to secure your environment?

Original template used by permission of Corporate Visions, Inc..

5. z SYSTEMS



Organizations that deploy highly securable z Systems have protection built-in **<Write "z Systems">**. The clients can address security requirements such as identity and access management, hardware and software encryption, and event logging and reporting. These capabilities have made IBM mainframes the platforms of choice for high-targeted industries. **<Write "z/OS" under " Operating Systems">** This is especially true for applications running under the z/OS operating system.

With features such as encryption assisted processors which allows you to encrypt your data without out impacting overall system performance. . **<Draw "Check Mark" beside Processor>**

The Hypervisor on the z System is the only one to have received the United States Department of Defense security level certification of EAL5. . **<Draw "Check Mark" beside Hypervisor>** The Operating System works with the hardware's storage protection to prevent one application from corrupting (or breaching) the data of another application. **<Draw "Check Marks" beside "Operating System" and "Applications">** All levels of storage from memory to DASD storage and even to the

data on tape backups are protected. . **<Draw "Check Mark" beside Storage>** It is because of these features that we say security on z Systems is "built in" not added on.

Today, z Systems is considered more securable than any other system. **<Write "SECURABLE">** Because of this**,** customers with a mainframe tend to have 80% of their critical data and production applications running on z Systems**.** **<Write "- 80%">**

QUESTIONS TO ASK:

- Where is your mission-critical data stored?
- What about mobile? Are clients able to connect directly to CICS® or IMS™ or do they go through the cloud or a web server?
- How is your z Systems environment connected to other systems that host your web and mobile applications?

NOTE TO PRESENTER:

POTENTIAL OBJECTIONS & RESPONSES:

OBJECTION: To our knowledge, our z Systems environment has never been hacked.

RESPONSE: z Systems environments are clearly the most secure commercial environment available. But our analysis of customers has identified vulnerabilities when those customers' systems are not configured properly. Another issue we find is that the largest threat our customers have is, in fact, an internal threat.

OBJECTION: Our z Systems environment is not connected to the Internet in anyway. Therefore, we are comfortable with our z Systems security program.

RESPONSE: If in your environment you have a server connected to the internet and in turn request and receives data from a z System, there is an exposure that it could be breached. This is why we feel that every enterprise should take a holistic view of their security strategy which would include the z Systems and distributed processors. We will talk more about this shortly.

OBJECTION: Is the added cost of the z Systems worth it?

RESPONSE: What is the cost of a breach? What is the cost of running your critical systems on a system that is not as secure as it could be?

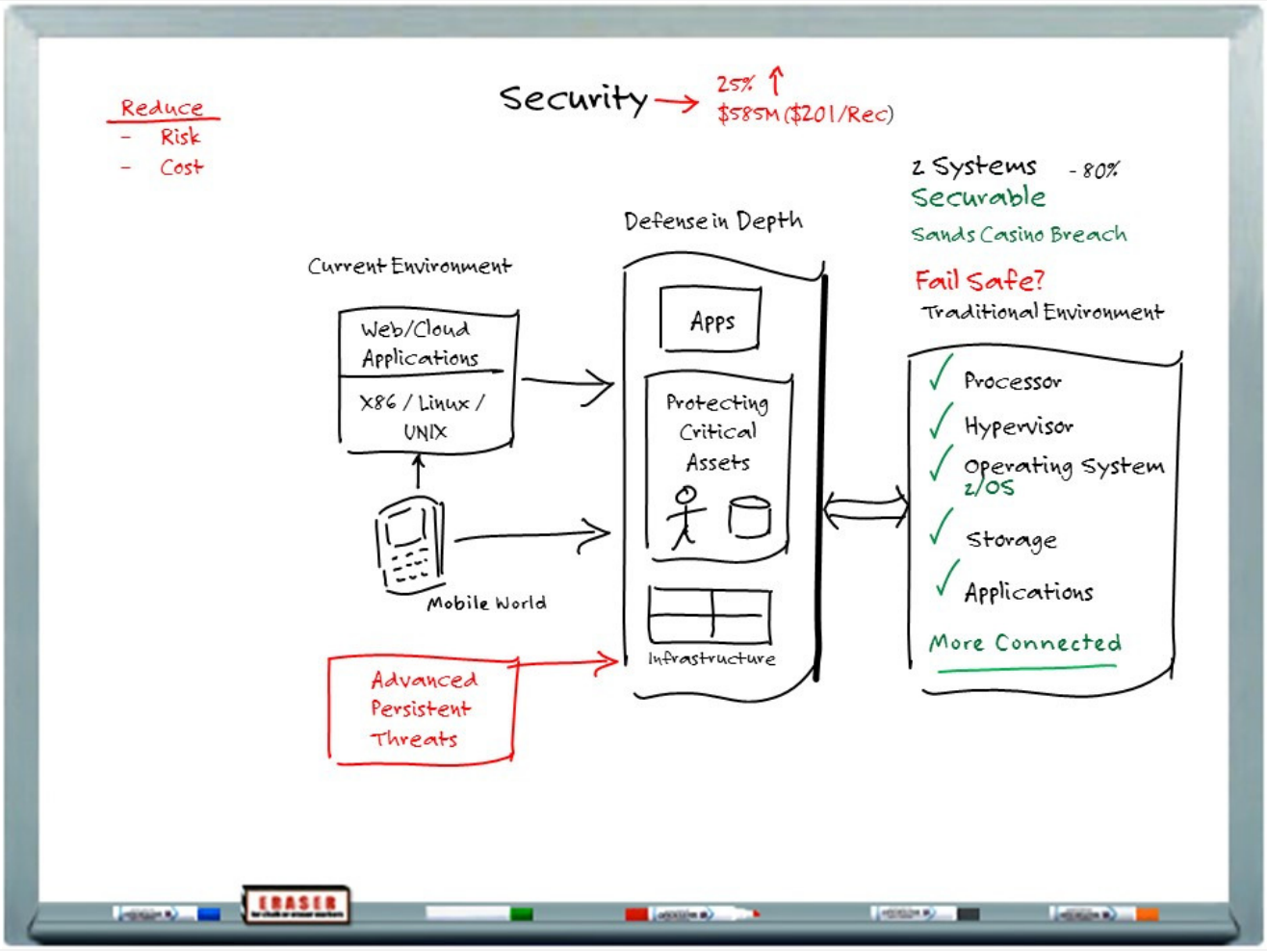
OBJECTION: Security of our z Systems environment is managed separately from the rest of our organization.

Original template used by permission of Corporate Visions, Inc..

RESPONSE: Many of our customers are recognizing that they need to take a more holistic approach to securing their overall IT environment. They are recognizing that a vulnerability anywhere in their environment is a threat to anything else in their environment, including their z Systems environment.

Original template used by permission of Corporate Visions, Inc..

6. FAIL SAFE



Recently, in the middle of the night, Sands Casinos (in multiple locations) noticed a breach occurring. They had people in all the casinos unplugging their x86 servers from the network. But their mainframe was never affected. **<WRITE: "Sands Casino Breach">.**

<WRITE "FAIL SAFE?"> So, can we consider z Systems to be inherently secure? When the z Systems were batch and transactions systems with very controlled access to the outside world, I would say "yes." But today, z Systems are more connected with the outside world. **<WRITE: "More Connected" at the bottom of the box>** z Systems is still the safest system, but with these connections through the web, cloud (particularly the public cloud) and the mobile world, z Systems is more susceptible to breaches than in the past. So, you need to look at how you can best protect your data and applications. This is where the layer approach of Defense in Depth comes into play.

Original template used by permission of Corporate Visions, Inc..

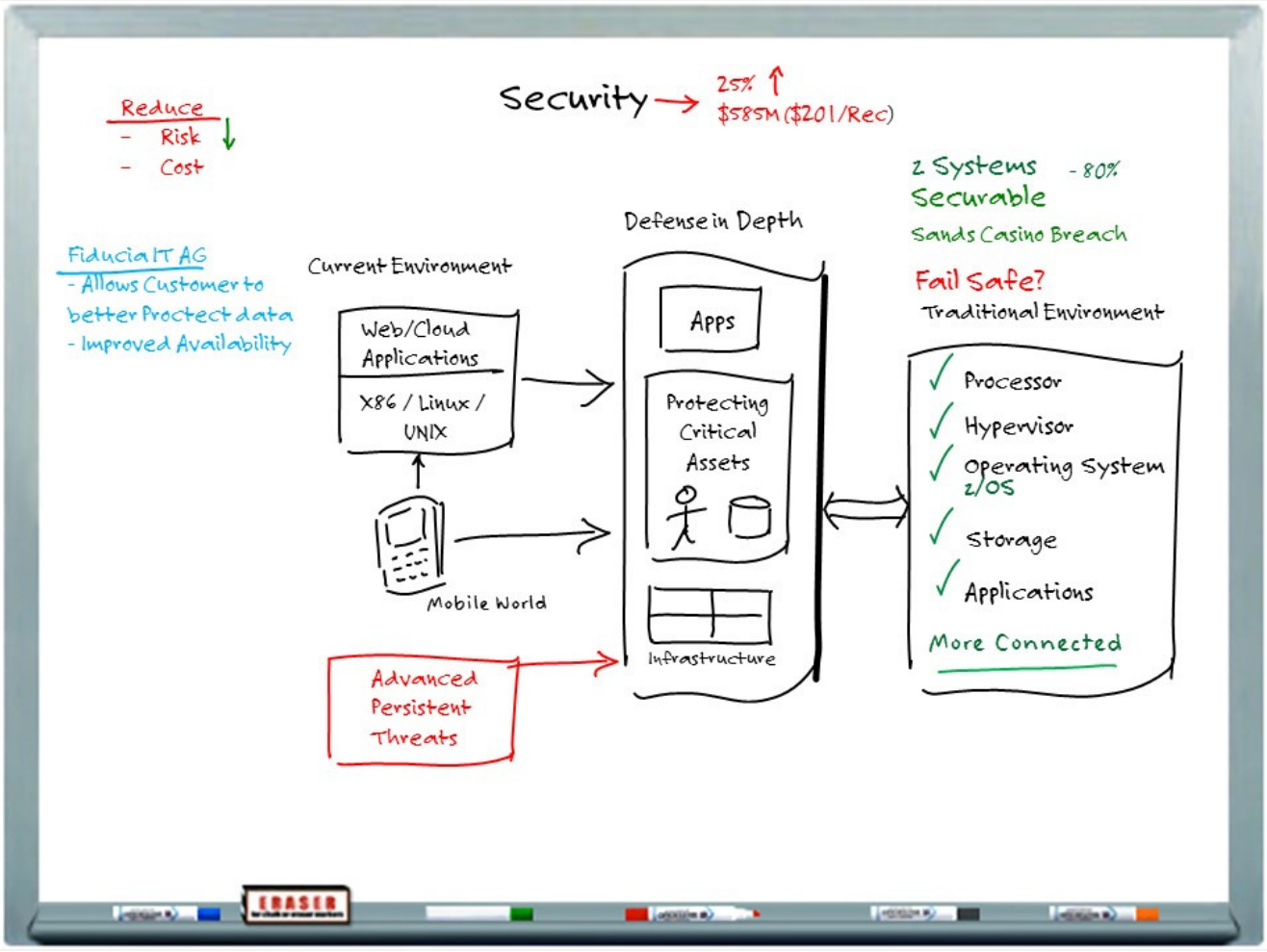
POTENTIAL OBJECTIONS & RESPONSES:

OBJECTION: This example seems to imply that a z Systems environment can't be breached. If so, then why are we having this discussion?

RESPONSE: In this example, if the casino had not disconnected their x86 servers, they might have exposed a pathway from those servers to their z Systems environment. To reinforce, we are advising our customers to take a holistic approach toward IT security, to consider all of the possible attack vectors, and to implement multiple layers of security controls to provide effective protection.

Original template used by permission of Corporate Visions, Inc..

7. REDUCED RISK CUSTOMER EXAMPLE



In a report by Clabby Analytics – "IBM System z – When Failures and Breaches Are Not an Option". Here are just a couple of them.

<WRITE: "Fiducia IT AG" and DRAW a line under it> Fiducia IT AG, a German IT service provider was deploying a new system. For their customer, the system had to be stable and, most of all, secure in order to protect the customer's data, **<WRITE: "Allows customers to:" and under that, write "- Better Protect Data">** they choose z Systems. Not only did z Systems reduce their risk, but by deploying it on z Systems, the availability of their systems increased. **<WRITE: "- Improved Availability">**

Here is an example of a client who has reduced their risk. <DRAW down arrow beside Risk>

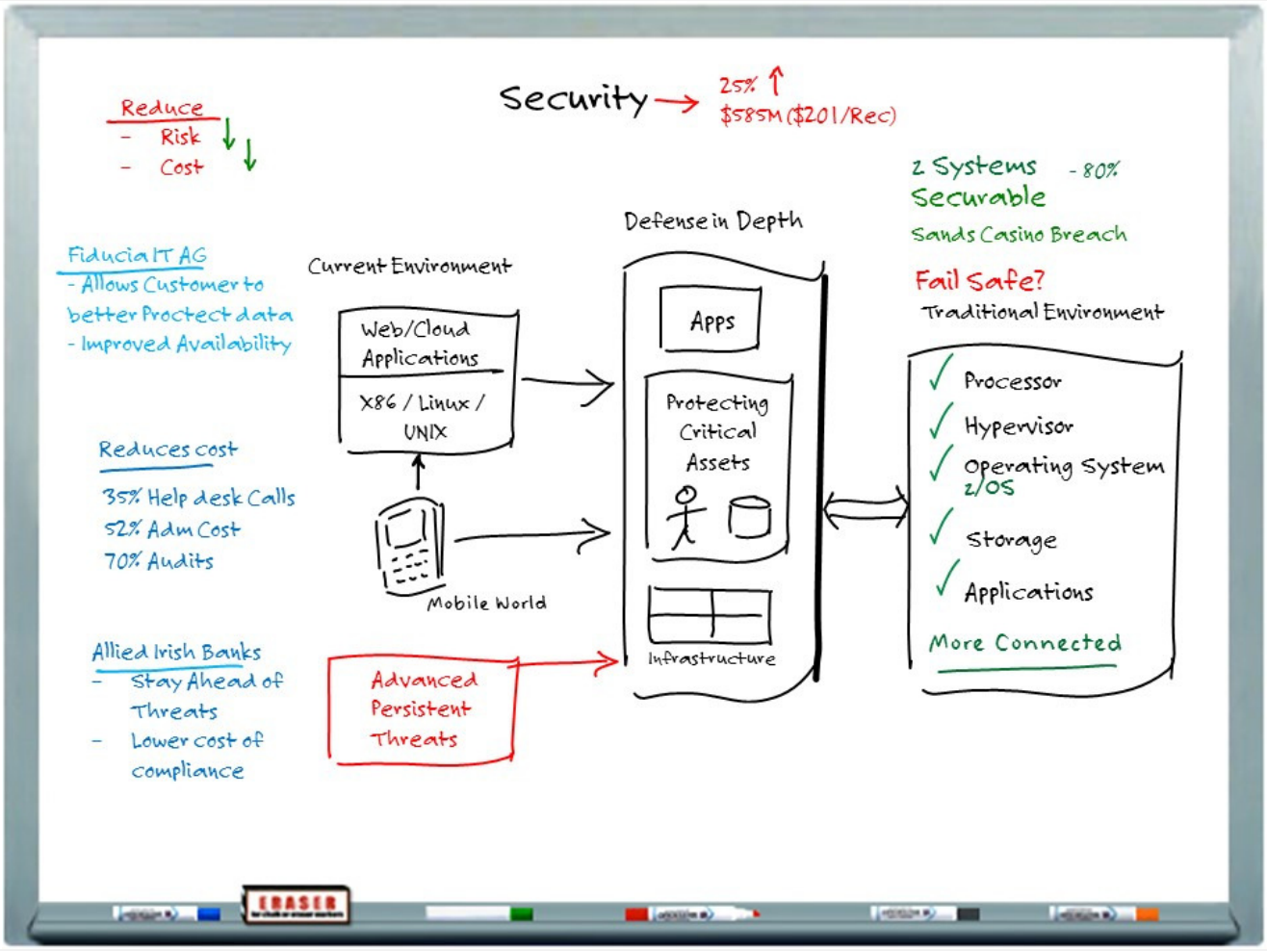
OBJECTION:

Again, if a z Systems environment is so secure, why do I need to do more?

RESPONSE:
To reinforce our earlier comments, a native z Systems environment is indeed very secure, but it can be compromised by misconfigurations and other inadvertent over-per missioning.

Original template used by permission of Corporate Visions, Inc..

8. REDUCED COST CUSTOMER EXAMPLE



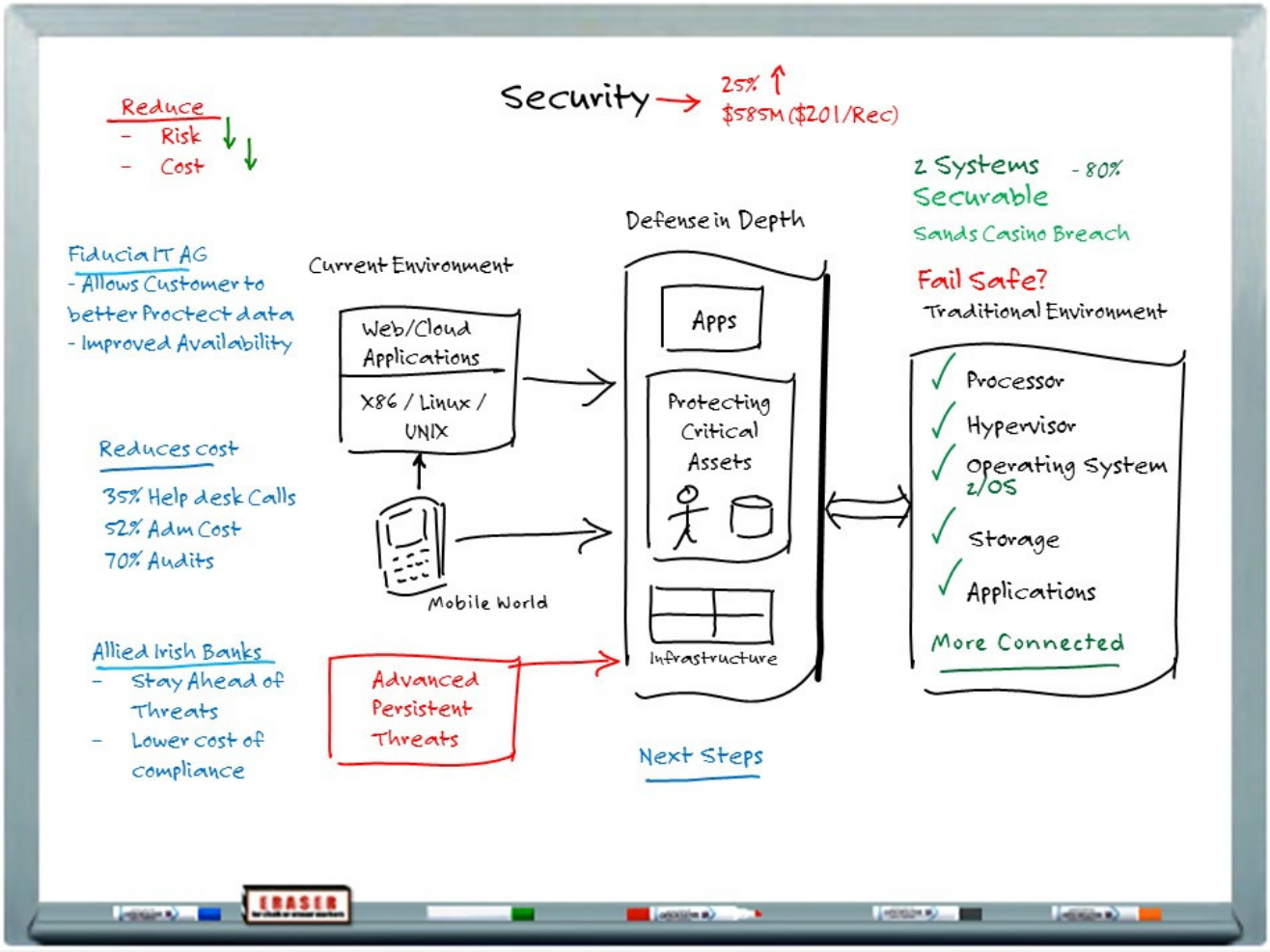
Like you, many customers are looking for solutions that will reduce their costs. A survey showed that the solutions deployed on z Systems reduced help desk calls by 35%. <WRITE: “Reduces Cost” and underline it, then under it WRITE “35% Help Desk Calls”>. Reduced administration cost by 52%. <WRITE: “52% Adm Cost”> And, reduced the cost of audits by 70%. <WRITE: “70% Audits”>

What industries are under more scrutiny today than Financial and Retail?

Here’s an example -- Allied Irish Bank headquartered in Dublin. AIB replaced their existing mainframe security software with the IBM Service Management solution which included RACF and zSecure. These help them stay ahead of security threats <WRITE “- Stay Ahead of Threats”> and lowered the cost of compliance <WRITE: “Lower cost of compliance”> with legal and regulatory requirements. They are able to monitor their environment in real time for configuration errors, exposures, and intruders. With the comprehensive and customizable reports, they reduce the cost to audits, while addressing the regulatory requirements. <DRAW: down arrow next to Cost under the Reduce heading>

Original template used by permission of Corporate Visions, Inc..

9. NEXT STEPS



So, how can z Systems help you better deal with some of the challenges we outlined earlier? How can z Systems help you reduce the risk you have today with your security? Security for z Systems is based on the most secure hardware with built-in security features. And to add to this we have RACF and QRadar which work together to give you the best security possible, today. But, while this solution of both hardware and software is the best in the marketplace today it is not fail safe. However, these should help you stay ahead of the breaches.

<WRITE: “Next Steps” and DRAW Line under it> Here is what I recommend for next steps. <WRITE under Next Steps what you have determined to be the best option going forward.>

NOTE TO PRESENTER: Prior to presenting this whiteboard to your customer, you should have reviewed the options available to you regarding what should occur next. At this point in the presentation, you can discuss the best options you have to offer them and when you and customer have agreed to the best “Next Step”, write that option on the board under Next Steps.

Original template used by permission of Corporate Visions, Inc..

Original template used by permission of Corporate Visions, Inc..

Appendix:

Next Steps Options

Visit http://www-03.ibm.com/systems/z/solutions/security_solutions.html click on the Integrity tab to learn more about z Systems integrity and how you can enhance it.

Access End to End Security with z Systems from the IBM Redbooks® series: http://www.redbooks.ibm.com/abstracts/redp5153.html?Open.

Visit http://www-03.ibm.com/software/products/en/category/security-framework to learn about the broad range of solutions that IBM can offer to help you enhance the security of your enterprise IT environments.

Performing a health check of your z Systems environment. You need to talk to your Security Specialist concerning this before offering to your customer.

Arrange for a presentation of IBM's End to End Security solutions for z Systems with your Security team.