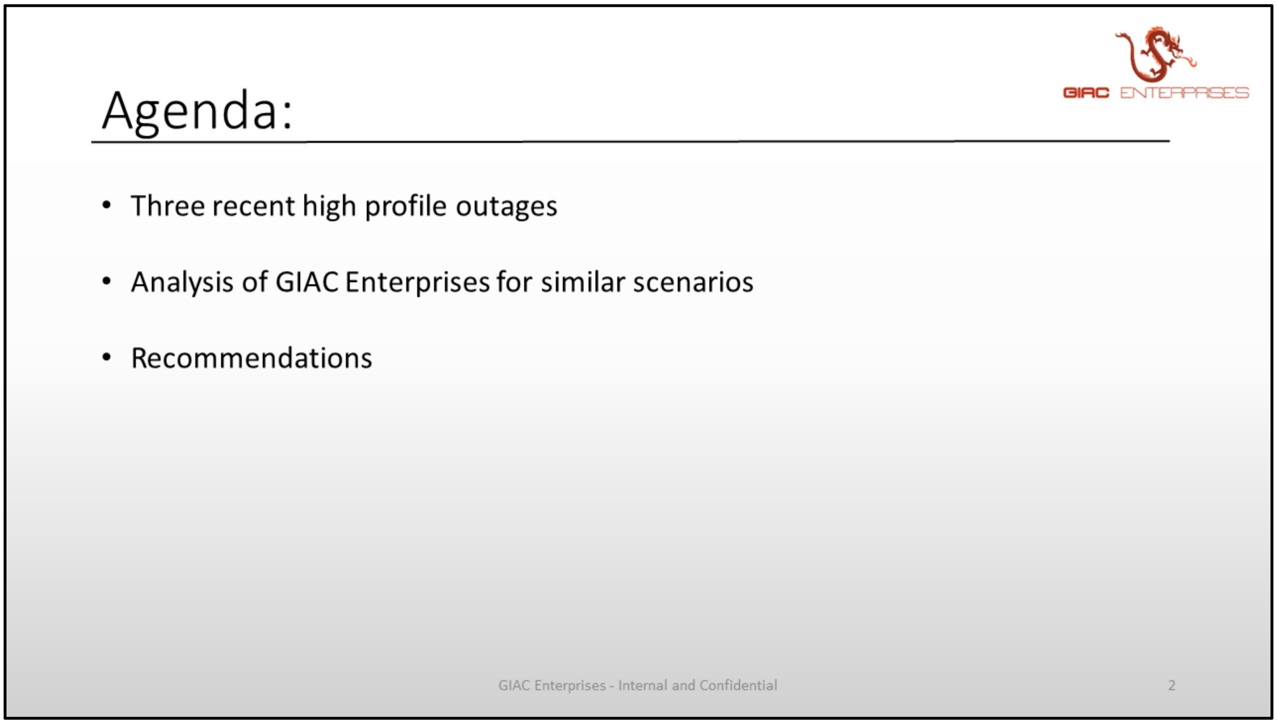
GIAC ENTERPRISES

Incident Response Preparedness Summary

(Prepared in response to several recent high profile outages)



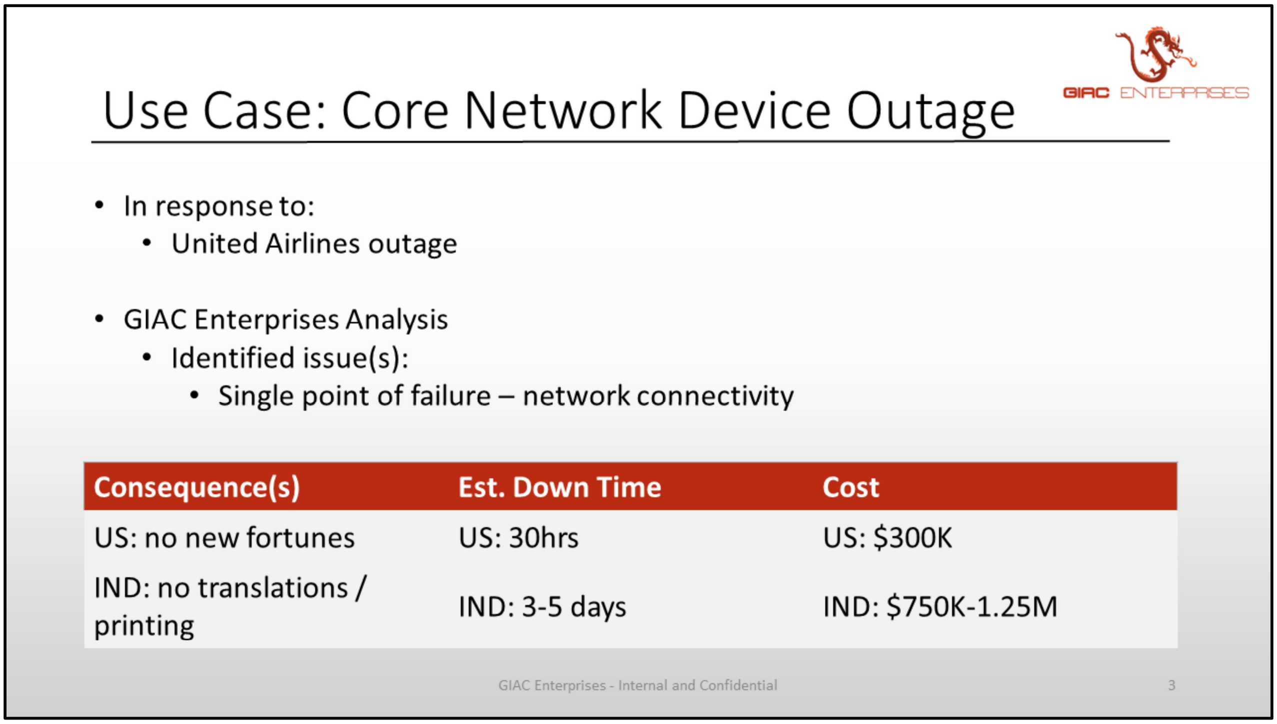
Agenda:

- Three recent high profile outages
- Analysis of GIAC Enterprises for similar scenarios
- Recommendations

In light of three recent high profile public outages, the IT Security Group reviewed the causes and impacts of those events and analyzed our environment to identify areas for improvement that would help prevent or minimize impact, should a similar event occur at GIAC Enterprises.

Surprisingly, each of these outages occurred the morning of July 9, 2015. Our analysis includes estimated impact, downtime, and costs associated with each scenario, as well as recommended solutions.

It should be noted that all three incidents were found to be caused by human or system error and were not associated with malicious activities. But during the course of our analysis, we developed Incident Response Preparedness checklists to assist the System Administrators and Incident Response Manager in determining if an event was caused by malicious actors or simply a mistake.



Use Case: Core Network Device Outage

- In response to:
  - United Airlines outage
- GIAC Enterprises Analysis
  - Identified issue(s):
    - Single point of failure – network connectivity

Consequence(s)	Est. Down Time	Cost
US: no new fortunes	US: 30hrs	US: $300K
IND: no translations / printing	IND: 3-5 days	IND: $750K-1.25M

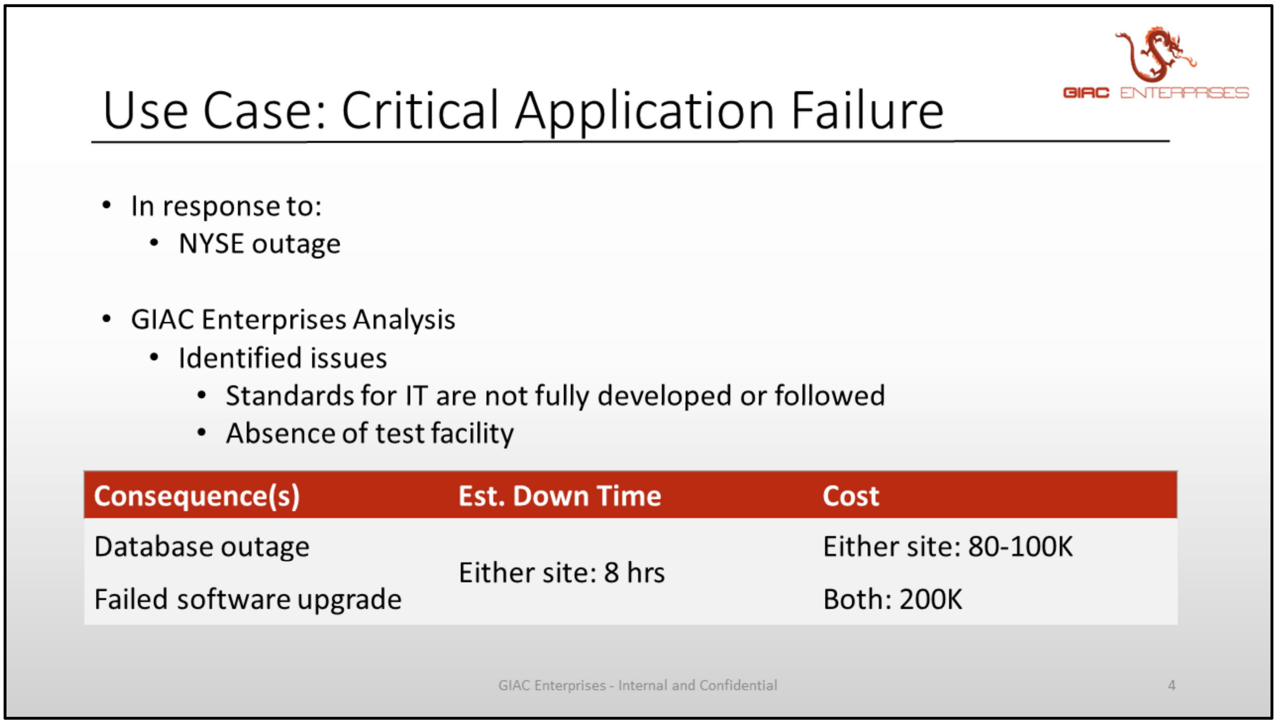
GIAC Enterprises - Internal and Confidential 3

The first use case was in response to the outage suffered by United Airlines on July 9 of 2015.

United suffered a hardware failure on their core network router, which caused the cancellation of 59 flights and a delay to over 1,000 flights. This also incurred significant financial and brand impact.

As a result, we examined the network infrastructure for GIAC Enterprises and found a similar single point of failure item in our own core router in both our US and Indonesian locations. Should this device fail in the US, it would prevent new fortunes from being generated. If the event occurred in our Indonesian facility, it would disable our ability to translate or print fortunes, thus preventing order fulfillment.

The downtime from this event would be roughly 30 hours in the US, at a cost of $300k. An Indonesian incident of this category would generate an outage of 3-5 days, costing $750k – $1.25M.



Use Case: Critical Application Failure

- In response to:
  - NYSE outage
- GIAC Enterprises Analysis
  - Identified issues
    - Standards for IT are not fully developed or followed
    - Absence of test facility

Consequence(s)	Est. Down Time	Cost
Database outage	Either site: 8 hrs	Either site: 80-100K
Failed software upgrade		Both: 200K

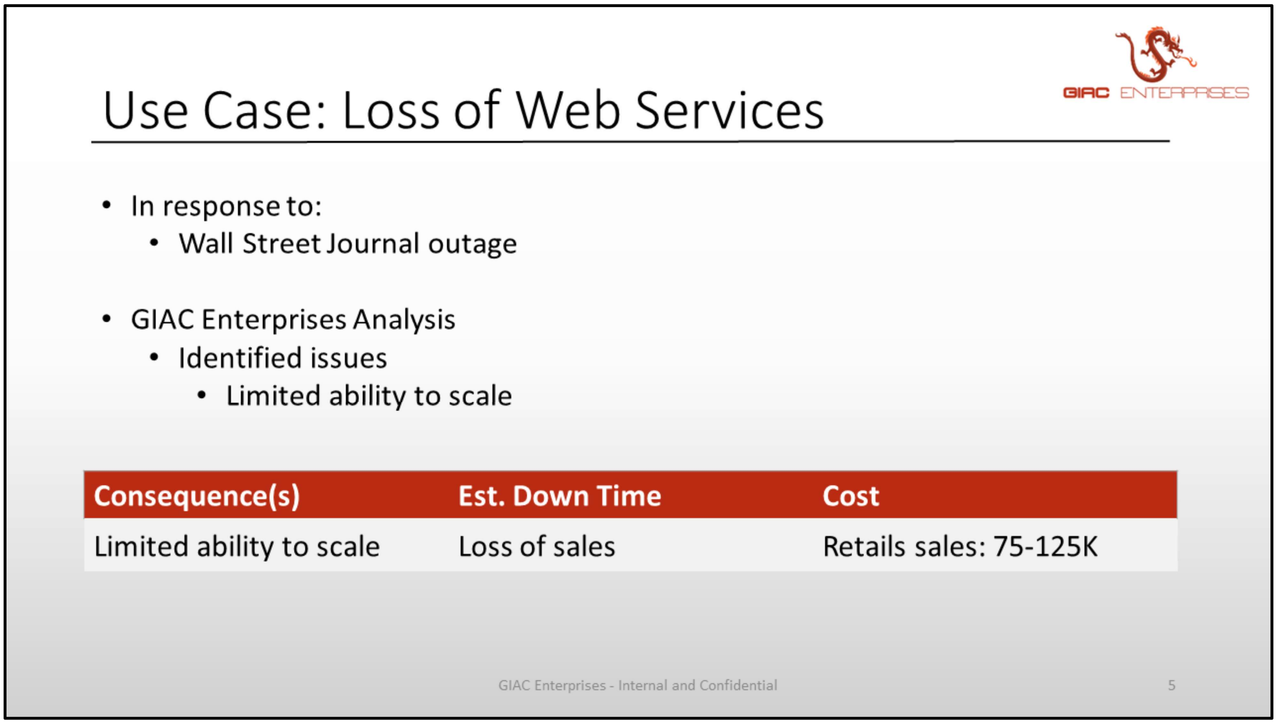
GIAC Enterprises - Internal and Confidential 4

The second use case was in response to the outage suffered at the New York Stock Exchange the morning of July 9 of 2015. (Yes, the same day as the outage at United.)

NYSE was implementing a new version of software prior to the market opening. The upgrade introduced communications issues and halted trading for 4 hours. The distributed nature of the market exchanges allowed traders to migrate to alternate exchanges, which helped to minimize the financial impact of the outage.

We examined the application architecture for GIAC Enterprises and discovered that IT standards are lacking in completeness and inconsistently followed. In addition, there is insufficient facilities to test new versions of our application prior to deployment to production.

An failed upgrade at GIAC could introduce downtime of up to 8 hours, costing $80k - $100k per location.



Use Case: Loss of Web Services

- In response to:
  - Wall Street Journal outage
- GIAC Enterprises Analysis
  - Identified issues
    - Limited ability to scale

Consequence(s)	Est. Down Time	Cost
Limited ability to scale	Loss of sales	Retails sales: 75-125K

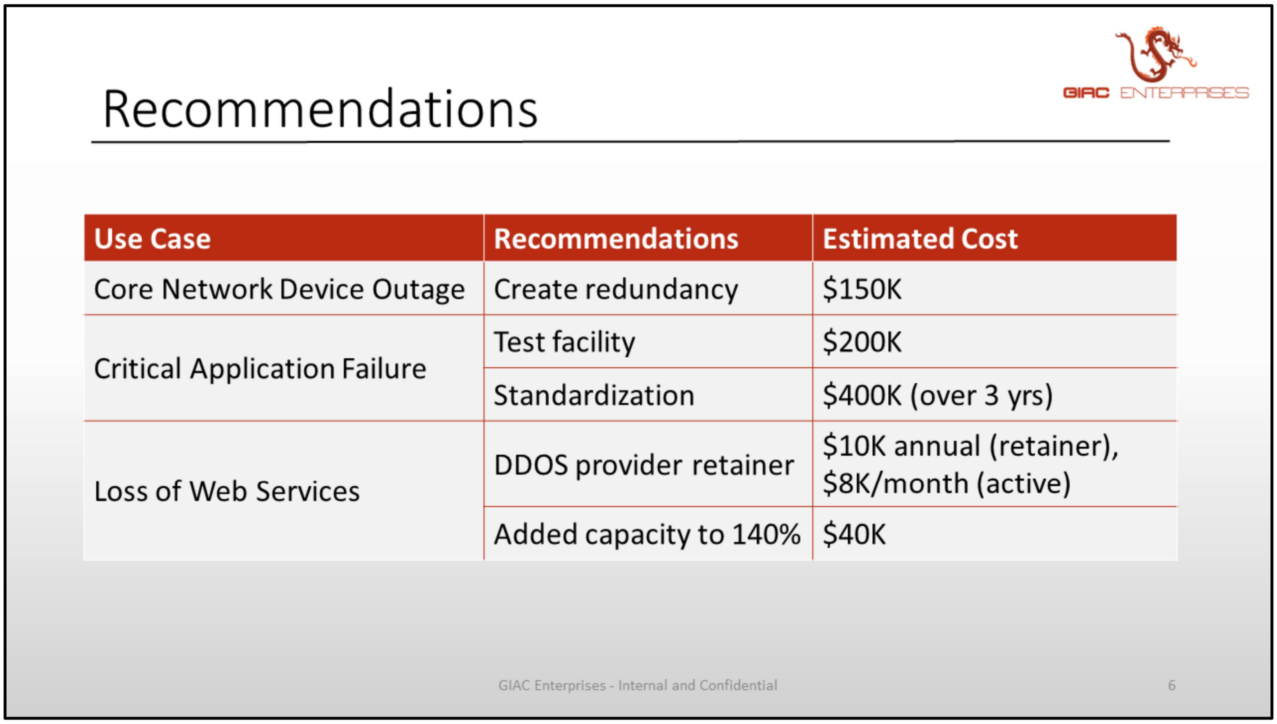
GIAC Enterprises - Internal and Confidential 5

The final use case we developed was in response to the website outage at the Wall Street Journal.

A full post-mortem of the event has not yet been published by Dow Jones, the parent company of the WSJ, but industry best guesses suggest their servers experienced an overload of traffic, possibly even related to the other two events occurring the same morning, which caused the webservers to stop responding in a timely fashion.

WSJ responded relatively quickly and was able to publish a placeholder page about 1 hour after the problem began, helping to reduce the load until the servers could recover. But their lack of any other communication has hampered further analysis or understanding of the event.

IT Security examined the web infrastructure of GIAC Enterprises and found that it is well designed, with the ability to load balance between our US and Indonesian facilities, but has only limited ability to scale up quickly, should traffic increase beyond 120% of normal capacity. Any increase beyond that would result in potential loss of sales until capacity could be sufficiently increased. This could take anywhere from 3-5 hours, with estimated costs between $75k and $125k.



Recommendations

Use Case	Recommendations	Estimated Cost
Core Network Device Outage	Create redundancy	$150K
Critical Application Failure	Test facility	$200K
	Standardization	$400K (over 3 yrs)
Loss of Web Services	DDOS provider retainer	$10K annual (retainer), $8K/month (active)
	Added capacity to 140%	$40K

GIAC Enterprises - Internal and Confidential 6

IT Security recommends the following 5 projects to help reduce the likelihood and impact of an outage similar to any of the scenarios we examined:

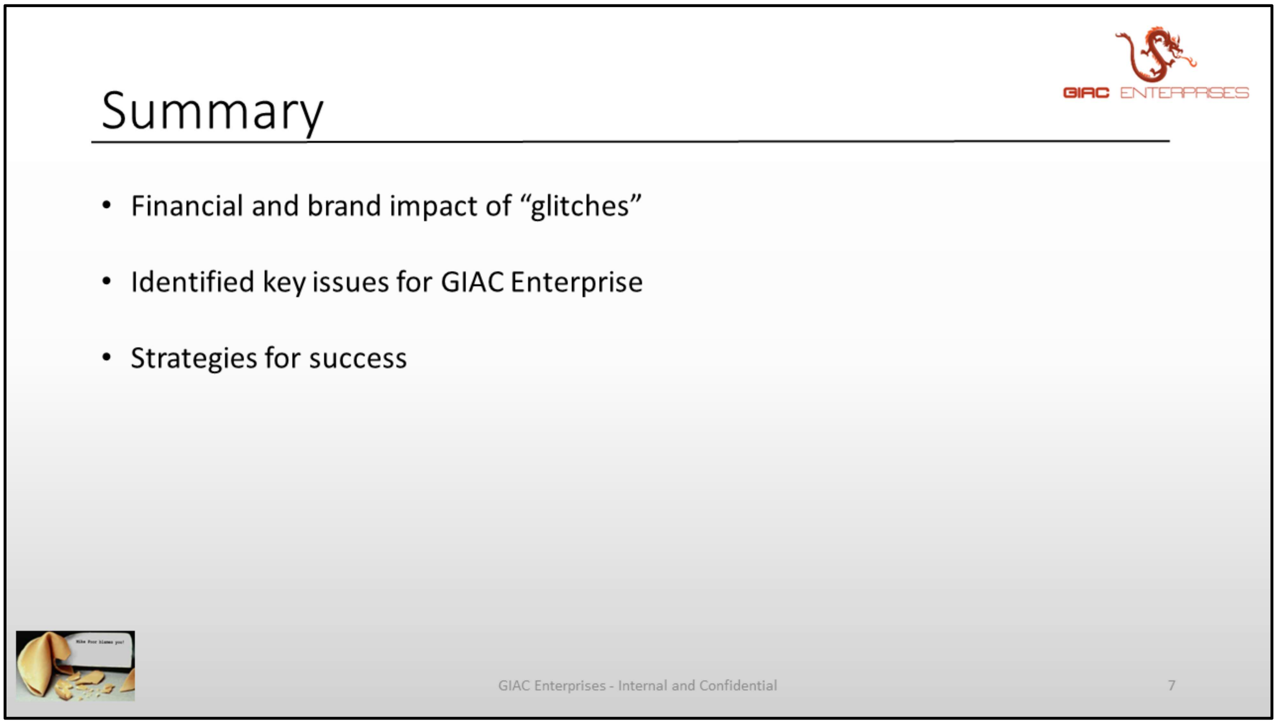
1) Introduce redundancy capabilities in the core routers of both the US and Indonesian facilities. This would take approximately 4 months and cost $150k

2) Create a test facility to validate new application versions prior to deployment to production. This would take approximately 6 months and cost $200k.

3) Update existing hardware and software versions across the data centers to comply with existing organizational standards. This effort would cost $400k, and be spread across 3 years.

4) Establish a retainer agreement with a DDoS Protection Provider. This would allow us to siphon off attack traffic against our ecommerce sites, while continuing to serve legitimate customers. These retainers typically cost $10k/year, but will increase to $8k/month should an attack actually occur.

5) Expand our ecommerce capacity to handle an additional 40% of traffic. There is no fiscal return for adding additional capacity beyond that at this time.



GIAC ENTERPRISES

Summary

- Financial and brand impact of “glitches”
- Identified key issues for GIAC Enterprise
- Strategies for success

Mike Poor blames you!

GIAC Enterprises - Internal and Confidential

7

After three recent high profile public outages, the IT Security Group for GIAC Enterprises reviewed the financial and brand impacts of “glitches” caused by system or human error, and applied those lessons learned to our own infrastructure.

Based on those lessons, we have a small list of recommendations to improve the overall security posture and business continuity of the organization.