BBGV
BRITISH BUSINESS GROUP VIETNAM

EUROCHAM
European Chamber of Commerce in Vietnam

AMERICAN CHAMBER OF COMMERCE
VIETNAM

Website Security in Vietnam

Survey Results and Best Practices

Prepared by:
Jim Fitzsimmons
MF8 International

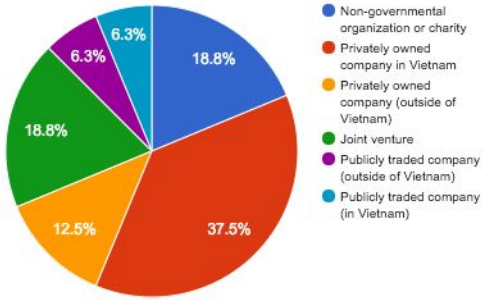
trg

a research project of TRG International and MF8 International

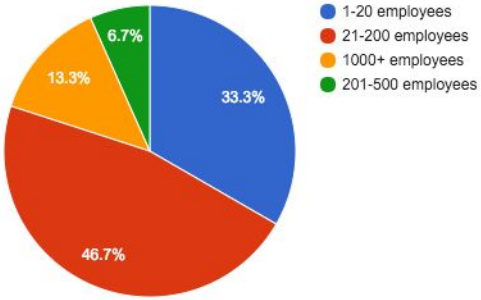
mf8 international

About Survey Respondents (17 Total)

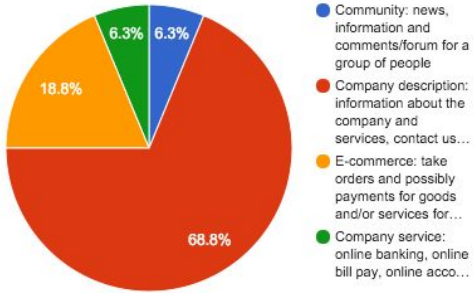
What Best Describes Your Company?



Number of Employees



What is the Website's Purpose?



Different Websites, Different Risks & Threats

Company Information
Customer Services
Internet Services
e-Commerce
Social Network
News
Personal Content
Community
Online Service

defacement

denial of service

data theft

malicious software hosting

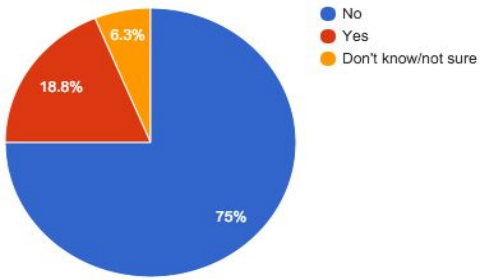
the hacktivist

the criminal

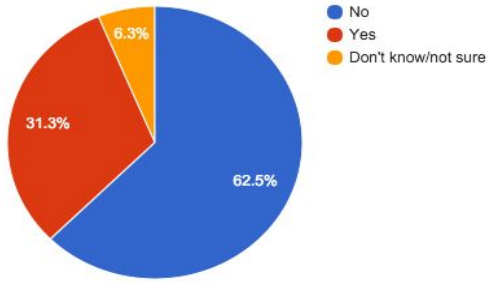
the spy

About Attacks on Respondent Sites

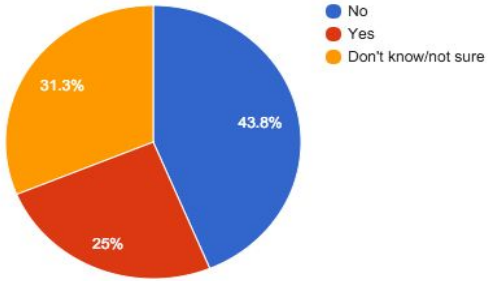
Has your website ever been defaced?



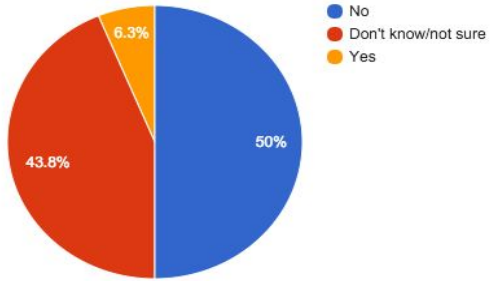
Has your site ever had a DOS attack?



Has malicious software ever been installed on your site to attack your users?



Has data ever been stolen from your site?



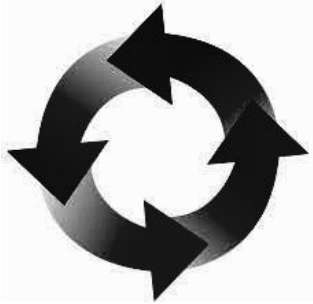
Operations & Security

your staff & service provider staff

your data center

Regulation, industry standards, best practices & policies for a security framework

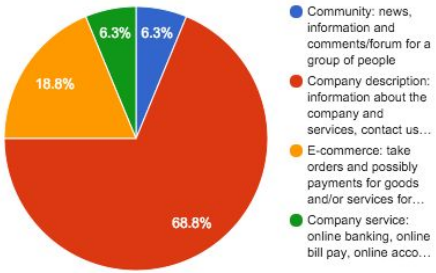
the software development lifecycle



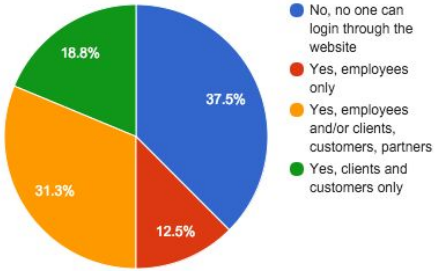
the cloud

About Survey Respondents' Websites

What is the Website's Purpose?

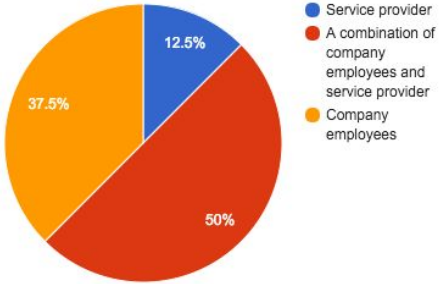


Can People Login to the Website?

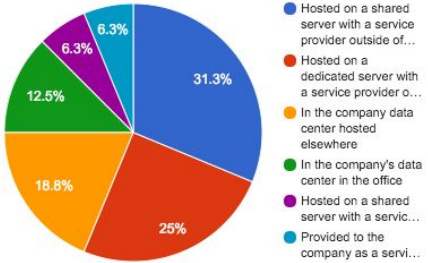


*note that only 1 respondent uses multi-factor authentication

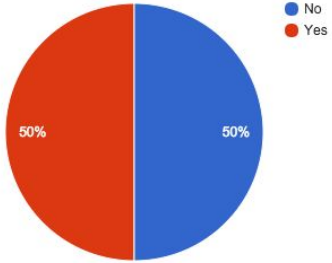
Who Maintains the Website?



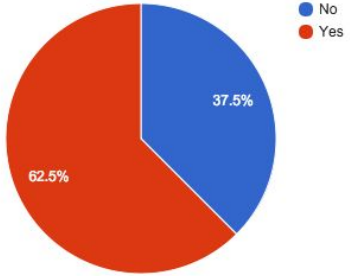
Where is the Website Hosted?



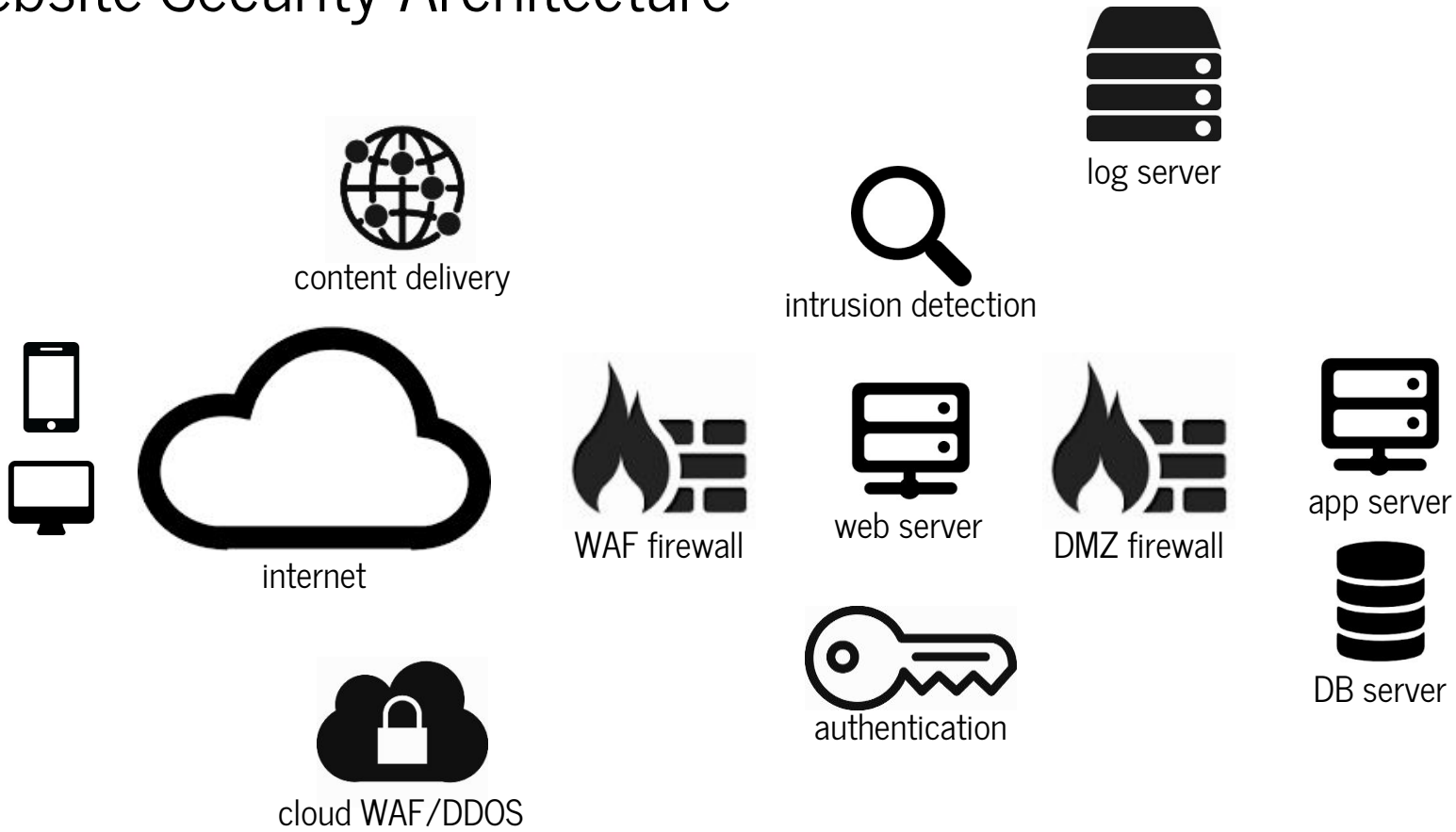
Does the Website Have Information on Employees, Customers, Users, etc.?



8. Do you have a security policy for the secure implementation and operation?

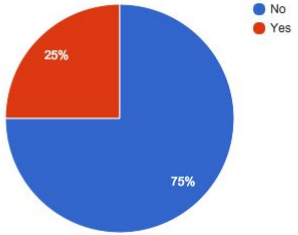


Website Security Architecture

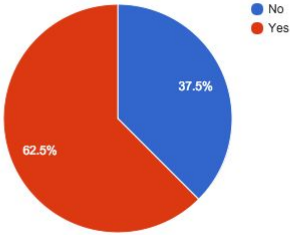


Respondent Security Architecture

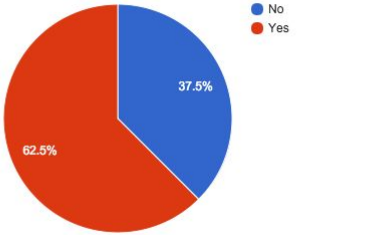
Is the site HTTPS only?



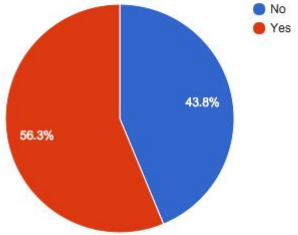
Do you use any tools or services to le impact of denial of service attacks?



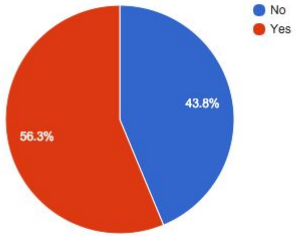
Are your web servers in a firewall-isolated DMZ?



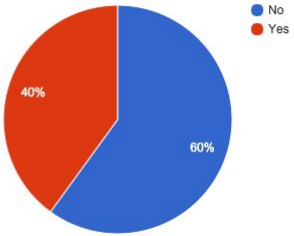
Is there a DMZ firewall between the web and other servers?



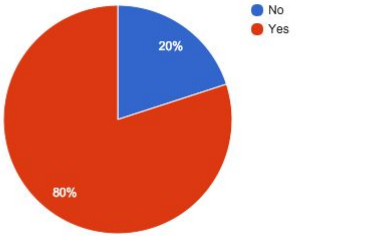
Do you use IDS/IPS?



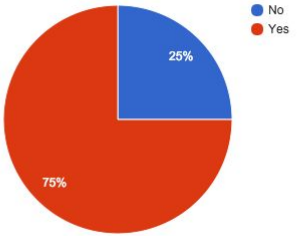
Do you use a WAF?



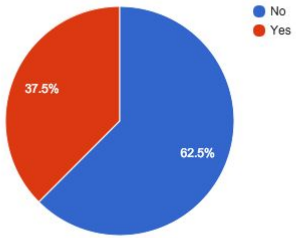
Do you monitor for unauthorized changes to the site and code?



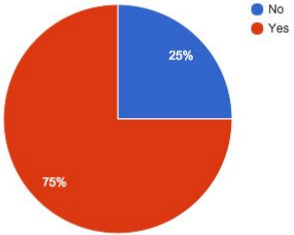
Do you scan the site for known vulnerabilities and misconfigurations?



Have your site had a pen test?



Did you test the website security for session IDs, authentication and access control?



Logging and Security

threat intel

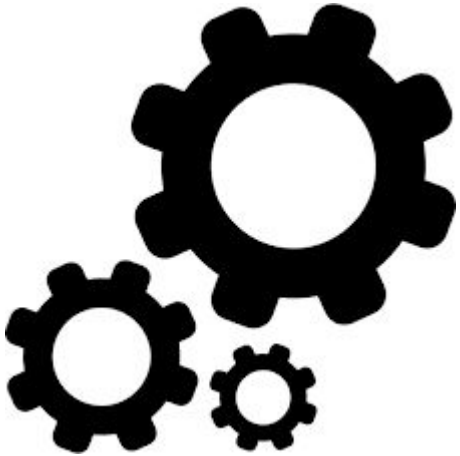
intrusion detection

content delivery

app server

cloud WAF

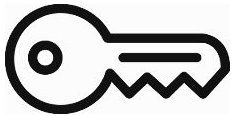
DB server



analysis platform
to correlate data

WAF firewall

DMZ firewall



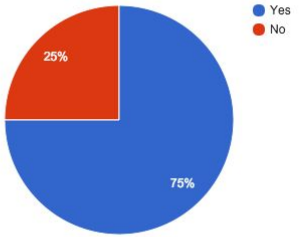
authentication

web server

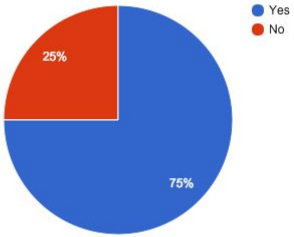
According to FireEye, successful attacks are discovered on average after 205 days

Respondent Logging & Security

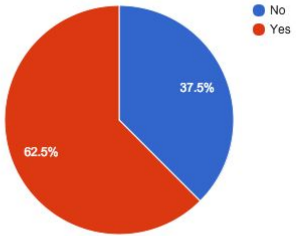
Do you collect logs of network traffic to and inside your site?



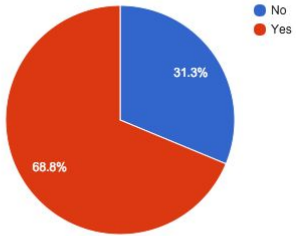
Do you keep logs of who accesses your website?



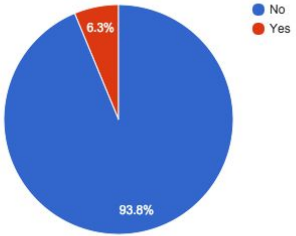
Do you collect logs from applications, databases, etc. in your website?



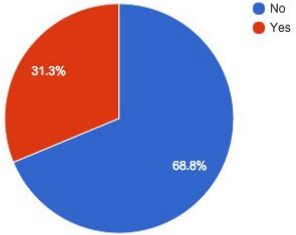
Do you collect logs for devices and servers in your website?



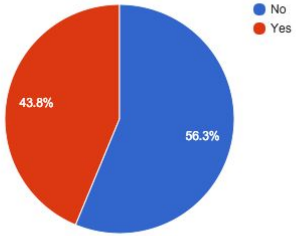
Do you store or stream your log data to a central console?



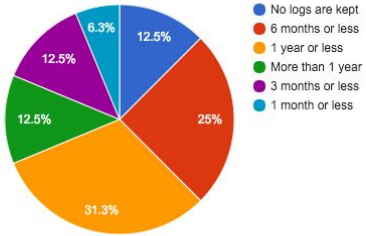
Do you have real-time security monitoring for your website?



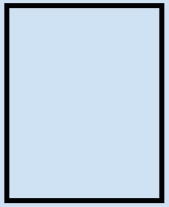
Do you collate the data from your logs for analysis and investigation?



How long do you keep your log files for?



Cheer Up, It's Easier Than You Think



API-enabled architectures

Inexpensive, orchestrated DEV environment

Container ready

Automatable security testing tools and config standards

Better physical security

Cloud-based security solutions

As highly available as you want to pay for