So the second session for this evening is on
security policies and standards this is part 2.

And our first question involves SQL injections - Your network
administrator wants to mitigate the potential risk of SQL injection
attacks as much
as possible. Which of the following is the best
route they could take? Take a moment
look at your choices and make your selections.

So we have lots of choices for answer C -
that is enable input validation and that is the
correct answer here. Applying host server OS
updates changing login passwords these are
not effective to mitigate SQL injection attacks
are neither is enabling HTTPS input validation is
in fact the way to mitigate the risk or potential
risk of SQL injections attacks as much as possible.

Let's move on to the next question -

All of the following are
true about an MOU except for what?
Which of the following statements
is not true about memorandum of understanding?
We have several responses in the
chat let's see what you're thinking.
Yes we have choices of B
So again
these statements all of these statements
about MOU are true except for one of them -
which one is not true.
So questions that involve
what something is not are
often a little more difficult
only from the perspective that we are so
used to studying what something is so
and the way this is worded makes it I think maybe
a little more difficult. All of the following
is true or are true about an MOU except
for what except one of these. So
memorandum of understanding is
typically a less formal agreement
so not legally binding. Do you think that
is a true statement or not a true statement?

You see another vote for B it's not
involved The Exchange so
not legally binding if that's true then
that's not the answer we're looking for.
Now even though it's a less formal agreement
it's still an agreement between two parties
so that statement's true what about does not
involve the exchange of money - is that true?

It's a less formal agreement
So typically with the exchange of money we're
looking at something contractual and signed by the
00:05:19.680 --> 00:05:27.420
appropriate parties so does not involve the
exchange of money that is a true statement about
MOUs that leaves us with the correct answer:
summarizes the work or responsibilities assigned.

Now looking back at the
chat a lot of you chose answer Choice B.

And we have sort of a question not sort of we do
have a question that is asking for the exception
so it's kind of you know a nut situation
but then you have that same situation and one
of the answers does not involve the exchange
of money so again you really need to be
careful when it comes to questions like this. Make
sure you read the question twice and make sure
you understand what you are being asked for and that's just good general
test taking tip, no matter

Let's let's move on to the next question -

An organization’s corporate
audit and security employees
need to investigate and discover any
discrepancies in employee activity.
Which policy should they enforce so that they
are able to complete this task with enough time?
Let's take a moment and look at the
answer choices and make your selections.
So we've had a couple responses
for Choice C access policies.
So we're looking for
discrepancies in employee activity
Anybody else want to weigh in
before we go over the correct answer?
So for this question the policy that
should be enforced is mandatory vacation policy
and this policy is sometimes used as a
security control. So what the intent is
is to sort of keep an individual from having
exclusive use of a system and by periodically
enforcing that the individual takes the vacation
they then relegate control of the system to
someone else. So it's a kind of detective
control and that is the correct answer.

So credential management is not the correct answer
these protections these policies for production
of credentials can sometimes involve you know
besides credential management. The strategies

can be eliminating vulnerabilities or securing employee devices teaching employees to recognize credential phishing attacks um administrator credential policy is also not correct.

This refers to admin accounts or root accounts right and the mandate that For example credentials are different from one system to another especially passwords so that if one account is compromised uh several others are not and then access policy defines the level of access for users so the correct answer here is mandatory vacation policy.

Let's go to the next question.

Ryan, one of your co-workers, has empty food wrappers soda cans and even stacks of sensitive customer data on his desk. What security policy is Ryan violating?
So there's a couple of answers that stand out is pretty obviously wrong. And then there's something in the question I think that leads you to the correct answer.

So we have several responses in the chat; let's see what you're thinking.

D, C, D, E, C. 1,2,3,4,5. So out of these five choices we had two votes for C, which is the correct answer: Clean desk policy.

So empty food wrappers soda cans and of course the the real giveaway here stacks of sensitive customer data on his desk. So yeah this is a violation of the clean desk policy. In fact it is the description is an antithesis of what a clean desk would be.

Next question -

The IT Department of Karen's organization decides to test their employees by sending out a phishing email with a malicious link that tracks whoever clicks on it. the results show that 87 of the 100 employees clicked on the fake URL. 87 percent.

What could have prevented that many people from falling for this attack?
This is another one of those questions I think that you really like to see. Because and I think that everybody agrees with me it's pretty obvious

and yeah yeah so this is this is a
situation of user security awareness

This is just one of those things that has to be
done certainly for people in the business that
is what all of you are intent upon doing, some things that we see all the time
are or become obvious because we have so
much exposure to them, but somebody whose job
is completely out of this field, it basically is
using the computer systems as a tool may not be as
aware and therefore it is up to you know the IT
Department to make sure that employees get proper
and not just inundated with training but the
proper user awareness training.

Let's move on to the next question.

Which of the following is not a necessary
procedure when off-boarding.
Thank you
So here again you're being asked
which one of these is not necessary.
We have about five responses in the
chat and let's see what people are thinking.
It looks like everybody's
voting for answer Choice C
Deactivate personal emails
and that is the correct choice
Disabling user accounts and privileges
is absolutely necessary um doing the best
that you can to make sure that whoever's being off-boarded is not in possession of information assets and then wiping employee-owned devices of
corporate data and applications these are all
common sense. It seems good and good things to do
certainly deactivating personal emails or contact
information - That’s the correct answer for
this question. Let’s move on to the next.

Which term describes a gamified training
event where learners must discover point
-based tokens within a live network
or scripted Q-n-A game environment?

I think this one's pretty obvious
too; it might even say that it's what
we're doing right now. So yeah, capture the flag
um and that's exactly uh what you're looking
at here with these questions they are point-
based and this is the Virginia Cyber Range CTF - fun stuff. Let’s move on to the next one.

Which security principle states that a

user should be allocated the minimum necessary
rights privileges or information to
perform his or her role and no more?

Lots of responses in the chat.
And for Choice B least
privilege and that is correct. This does
not involve a code of conduct or separation
of duties or standard operating procedures.
This is the principle of least privilege
So segregation of duties could look
like a correct answer; basically it ensures
that employees don't have access to systems that
will lead to conflicts of interest fraud or abuse.
So the correct answer again least privilege. Let's go on to the next question -
A company's employee just got a new social
media account they have a lot of friends
that work in the same field of business. What
is the biggest security risk in this situation?
Take a moment look at your answer
choices and make your selections.
So an employee gets
a new social media account
and they have a lot of friends that
work in the same type of business
so that's pretty much the big clue here.

So when it comes to security
what's the weakest link in the chain?
What do you think?
The end user - Sure, the human element, right?
And even if it is not malicious
What do we like to do? what do
we like to talk about with our friends?
And especially if they do what we do -
over-sharing talk about work what we
do may be something interesting that happened
So the answer choices - the
employee's email address will be added into
a database for random subscriptions - no not really a concern;
Answer Choice C - others can
see the employee's IP address while they're
at work using the social media account.

That's really not going to be representative
of a big security risk; an attacker can post on
the employee's account acting
as them - I mean that can be a problem.
It really boils down to sort of human
nature here; the employee could engage on
the site too much and expose the company's
intellectual property. I mentioned earlier that
the intent does not have to be malicious and I can

speak from experience to this point thinking back
to my early days as a software engineer and I was
working on a particularly interesting project for
a company called Flexible Manufacturing Systems
and we were engaged with building an autonomous

guided vehicles and you know this this was the
coolest thing I think I'd ever seen in my life.

This was in the mid-to-late ‘80s and this vehicle was just
off the chain, it was not guided by paint stripes
on the floor or wires buried in the floor.
Was free-ranging and it was just like I said the
slickest piece of technology I'd ever seen. and
you know so myself and some of the other software
engineers we'd go out after work and you know have
some something to eat and you know I mean it just
it just would come out I mean we talk about other
things but the first things that usually came from
Mouths were the events of the day or you know how
part of the project that we were working on was
turning out or maybe some of the challenges that we were coming across
and you know this was all done in in the spirit of you know camaraderie
and you know possibly even getting someone
else's opinion on you know what was going on.
But when I think back to this sitting in
in the restaurant having these conversations
sometimes they get quite animated and fact of the
matter is you don't know who's sitting around you
and you know maybe you know in the excitement
of having these great discussions with your
colleagues you know even though they work on other
parts of the project you could have been exposing
proprietary information and so there's no
malicious intent but you know that was human
nature to have these kinds of discussions.
So anyhow let's move on to the next question.

Which of the following is the information
security standard for organizations that process
credit or bank card payments ? So
hopefully everybody knows this one;
lots of responses very quickly.
And all for Choice D so D is correct.
PCI DSS payment card industry data security
standard set of security standards formed
in 2004 by Visa, Mastercard, Discover Financial
Services, JCB International, and American Express.
The standard is administered by the payment
card industry security standards council
and it's use mandated by the different
card brands so this is the correct answer.
IEEE - Institute of Electrical and Electronic
Engineers - that's a professional organization

not the correct answer statement on standards
for attestation engagements is a set of Standards
governing service organizations security
practices Choice B and that is not correct.
and then FIPS is federal information processing
standards refers to a series of computer
security standards developed by the federal
government United States federal government in
line with federal information security management
Act and approved by the Secretary of Commerce
so PCI DSS payment card industry data
security standard - correct answer.
A company that is located in Paris France is
complying with the GDPR when dealing with what
Take a second look at your
choices and make your selections.
So we have some choices in the chat - let's
see looks like we have votes for B,C and B.

Vulnerability assessments, personal data protection,
financial services, and separating workloads for
performance and load balancing. This is an
example of a more knowledge based question
the um key to this is understanding what GDPR is
and that is the general data protection regulation
this GDPR introduces rules for organizations
that offer goods and services to people in the
European Union so this is very much involved with
personal data protection so
again if you if you know that much of it then
you would go right to personal data protection.

Understanding that workloads separating workloads
for performance and load balancing balancing load
balancing and vulnerability assessments are you
know more technical answers not involved with this
financial services personal data protection
would be the remaining two but again understanding
a little bit about GDPR would lead you right to
the solution of personal data protection.

HIPAA - the date of privacy framework protects
health care data for which of the following?
It looks like they're all for answer D - all
options are correct so protecting personal
health care data for storage reading and data
in transit and, yes, all options are correct.

So that one's I think fairly easy as well. Let's move on to the next
question

as the corporate CISO - a new industry security
compliance certification you're pursuing - requires
that you implement a new corporate security policy

regarding smartphone usage for business purposes.
Before writing the policy
what is a good first step?
Take a second look at
the choices and make your selection.
So we've got some responses in
the chat; let's see what you're thinking - A B A A

So it looks like the bulk of the choices in
the chat are voting for get the
legal department's opinion first.

So we can look at answer Choice C which
states issue compliance smartphones to all
employees and that's definitely putting
the cart before the horse so to speak
pass the rough draft to the policy out to
the employees - no that's obviously wrong.

The question states before writing the policy
so C and D clearly wrong; A and B are the two
that you have to decide between and for
the Chief Information Security Officer,
You're going to be discussed with
management and get their write-off.
Because you need to have something to show the
legal department before you can get their opinion
and yes always important to ensure upper
management is on board and aware of policies
prior to creation well said so correct answer
is Choice B.

Now the next question

Which of the following is based
on STIX and TAXII standards?

Take a look at this and make your selection.

So as before with at least one
other question the one involving GDPR
you need to know what these
two clever acronyms stand for:
So STIX - structured threat information
expression - sticks if you will
TAXII or maybe we will just say trusted
automated exchange of intelligence information
so what are they involved with?
So we have a couple of responses
So we have three responses in the chat let's
see what's on your mind A, A and C
So the correct
answer here is automated indicator sharing.
And so basically um the structured

threat information or Stakes defines
the what if you will of a Potential Threat and
TAXII defines how the information is transmitted
and so the point here is to you know
make these things easily available
and so this is done because the um
outputs are machine readable automated
and can easily be integrated into systems now
when you look at this question and these responses.
one of these and I'm talking now about
answer Choice D vulnerability databases
hopefully you've seen this
enough that an organization
will come to mind fairly quickly when you
see that what organization am I talking about
so concerning vulnerability databases, I'm talking about the Miter Corporation
so you've got that
yes CVE - common vulnerabilities and exposures - that's miter
so knowing that you can eliminate Choice D pretty quickly that leaves
threat maps and filer
code repositories so file and code repositories
websites that contain a list of common exploits or
threats against product and they typically
publish the compose code or compiled files
so again not involved with STAKES and TAXI and
threat maps are what you can see just go by
going in and doing a search for you know real-time
attack maps or something of that nature
C,B,D right so automated indicator sharing is the correct answer.

Let's move on.

This looks like last
question for this section.
Which of the following statements below is true
regarding GDPR? We're going to revisit this
for a second - take a moment read your answer
choices carefully and then make your selections.
We've got several responses in the chat
There's two Votes for A, let's see.
and a couple more votes for a I have
a lot of people voting for A it seems
General data protection
regulation is a European Union
deal so A is incorrect; It applies to EU personnel
so A is not correct.
and B is not correct.
Choice C - GDPR applies to EU data
subjects but does not apply to
American companies that collect or process
the personal data of people in EU countries
this answer is stated is also not
correct but if we took out the word not

and we say GDPR applies to EU data subjects
and applies to American companies that collect
or process the personal data of people in EU
countries that would be a correct statement.
But for this question the correct
answer GDPR applies to European
Union data subjects that does not apply
to American data subjects;
so that perhaps up this section on
security policies and standards part two.